

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 525 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 2
 to
CONTRACT NO. 071B4300073
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR	PRIMARY CONTACT	EMAIL
Imagetrend, Inc. 20855 Kensington Blvd Lakeville, MI 55044	Trisha Moline	tmoline@imagetrend.com
	PHONE	VENDOR TAX ID # (LAST FOUR DIGITS ONLY)
	(952) 469-1589	-3871

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
PROGRAM MANAGER / CCI	DHHS	Marvin Helmker	(517) 241-3024	Helmkerm1@michigan.gov
CONTRACT ADMINISTRATOR	DTMB	Whitnie Zuker	(517) 284-7030	zukerw@michigan.gov

CONTRACT SUMMARY			
DESCRIPTION: Michigan Emergency Medical Services Information System (MEMSIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
April 1, 2014	September 30, 2019	5, one year	September 30, 2019
PAYMENT TERMS	F.O.B.	SHIPPED TO	
Net 45	N/A	N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF EXTENSION/OPTION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>		September 30, 2019
CURRENT VALUE		VALUE/COST OF CHANGE NOTICE	ESTIMATED REVISED AGGREGATE CONTRACT VALUE	
\$946,420.00		\$35,500.00	\$981,920.00	

DESCRIPTION:
 Effective June, 1, 2015 this contract is hereby INCREASED by \$35,500.00 to implement the Emergency Medical Services (EMS) License Management application otherwise known as "Payment Gateway Module for the Michigan Department of Health and Human Services (MDHHS), EMS Section per agreed upon Contract 071B4300073 Change Notice #1 and the attached Statement of Work.

Per Change Notice 1, the 9/11/2014 State Ad Board approved \$387,675.00. Actual Amount allocated to Contract for CN1 was \$225,300.00. Remaining value of the Ad Board authorized amount that may be added via Statement of Work is \$162,375.00. This Change Notice, 2, reduces the remaining value by \$35,500.00. New remaining value of the Ad Board authorized amount that may be added via future Statement of Work is now \$126,875.00,



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: EMS Payment Gateway Implementation CCN 2	Period of Coverage: 6/1/2015-09/30/15
Requesting Department: Michigan Department of Health and Human Services (MDHHS)	Date: 6/14/15
Agency Project Manager: Marvin Helmker	Phone: 517-241-3024
DTMB Project Manager: Russ Tiedt	Phone: 517-335-3288

Brief Description of Services to be provided:
Implement the Emergency Medical Services (EMS) License Management application otherwise known as "Payment Gateway Module" for the Michigan Department of Health and Human Services (MDHHS), EMS Section for time period 06/01/15 - 09/30/19 per agreed upon Contract 071B4300073 Change Notice #1.

Current Contract Value: \$946,420.00
Cost of Contract Change Request: \$35,500.00
Amended Contract Value: \$ 981,920.00

BACKGROUND:

DTMB has contract (071B4300073) with Imagetrend, Inc to provide maintenance/support and hosting for Emergency Medical Services (EMS) Michigan Emergency Medical Services Information System (MEMSIS) State Bridge, Visual informatics/Data Mining, and Patient Registry/Trauma Bridge for the Michigan Department of Health and Human Services (MDHHS).

The Michigan Department of Health and Human Services, EMS Section, currently licenses 28,000+ EMS personnel, and 820 EMS response agencies. Additionally, the Section is mandated to review and approve EMS education programs, provide oversight of Medical Control Authorities, conduct random audits of licensee continuing education records, and investigate complaints and allegations against EMS personnel. The Section presently uses the L2K system to manage several of its processes. The implementation of the Payment Gateway Module will create a more efficient method of payment and refunds by allowing the functionality of credit/debit card payments.

If not procured, current inefficiencies and services which are not customer-friendly will continue. These include the inability to eliminate the excess fees charged to the EMS section by MDHHS Casheiring for payment and invoice processing due to the requirement to maintain the L2K and K&L systems.

PROJECT OBJECTIVE:

ImageTrend will implement the requested payment gateway integration, create a new feature to allow for payment refunds, and provide legacy data migration services.

SCOPE OF WORK/TASKS:

The Contractor will implement the requested Payment Gateway Module integration, create a new feature to allow for payment refunds, and provide legacy data migration services. The Contractor will provide ongoing hosting and maintenance to support the Payment Gateway Module.

Technical support is required to assist with the following tasks:

As a part of this MDHHS Project, ImageTrend will be responsible for performing tasks throughout the various stages of this project. The following is a list of these tasks which will result in the successful completion of this project:

Development Services

- **Payment Gateway Integration**

- Michigan's License and Certification Management System will facilitate the secure transfer of information and users to the payment processor (MDHHS).
- The MDHHS will input payment information into the MDHHS sessions hand off interface to process the transaction.
- An interface within the public (non-administrative) side of Michigan's License and Certification Management System will be developed for users with access to make payments.
- An internal interface will allow administrative users the ability to view transaction number, transaction status, charge name, charge amount, payment method, and payment date.

- **Payment Gateway Integration Annual Support**

- **Payment Refund Functionality**

An internal interface will allow administrative users the ability to view:

- Transaction number
- Transaction status
- Charge name
- Charge amount
- Payment method
- Payment date

On this interface, MDHHS can initiate a refund for the transaction.

When the refund button is clicked, Michigan's License and Certification Management System will post a web service request and retrieve the refund data for the transaction identified by the associated token and display result on the payment page.

- **Legacy Data Migration Services**

- Import, map, and normalize legacy data consistent with the fields that are available in the ImageTrend data dictionary. Data dictionary is attached.
- Data will be accessible within the system based on the permissions provided to MDHHS.
- In the event that the data provided exceeds the amount of data that the MDHHS wants imported into the system, the MDHHS must indicate these thresholds. (I.e. if 10 years of data is provided, then 10 years of data will be imported unless otherwise guided).
- This assumes that the data will be provided in a format that is editable, excel, .csv, or database. Any legacy attachments that would need to be made available in the system must be provided with a file name that is unique to the file that they would be attached to within the ImageTrend system.
- This assumes that the data provided will include a data dictionary or at minimum definition to the fields. When a data dictionary is not available, then MDHHS will provide a subject matter expert to offer guidance on how the field should be mapped.
- Once the legacy data is imported, ImageTrend will provide notification and the MDHHS will have 30 days to review the data and provide feedback on what data is missing from the import. After 30 days, ImageTrend assumes that the data is valid and will dispose of any legacy data provided that is not stored in the system, excel, .csv, or database. MDHHS is responsible for validating the data in terms of the following key attributes: the relevance, accuracy, integrity, consistency, completeness, validity, timeliness, accessibility and compliance.
- When a field does not exist in the ImageTrend system or data dictionary, then alternative collection methods will be offered. When this does not meet the requirements of the MDHHS. Development would be required and a separate timeline and statement of work will be provided.
- The legacy imported data will occur a maximum of two times. The first time to provide a baseline of information as it will appear within the system so that the MDHHS may validate the data. A second time to provide any changes to the data from the time of original import. This second import should be scheduled as close to the go live to minimize any requirements for dual entries between the systems - old and new.

- Legacy data migration will include matching License Management accounts with the accounts in State Bridge or Elite based on criteria determined by the MDHHS.

ASSUMPTIONS:

- ImageTrend will use its computers, software, licenses and other materials to create and develop the module. ImageTrend is also responsible for operating and testing the software on the Contractors' systems and servers.
- ImageTrend has the right to develop and release this custom development as part of a regular product release containing other product features and fixes.

DELIVERABLES:

Deliverables will not be considered complete until the Agency Project Manager has formally accepted them. In addition to agreed upon deliverables in the Master contract 071B4300073, the following deliverables are to be provided:

EMS License Management Implementation Services

Payment Gateway Integration (Qty. 1)
Development of License Management Payment Feature (40 hours)
Legacy Data Migration (100 hours)

EMS License Management Annual Support Fees

Payment Gateway Integration Annual Support (4 years; beginning after being in a production environment without error (no service, reporting, hardware or software failures) for a period of 30 days.

Change Management

Contractor strives to completely assess all requirements and uses past implementation experience to ensure that project change requirements are minimized. Most changes are covered under support or version release policies. However, should a project change(s) be necessary, Contractor will follow the Change Management process of the Master Contract. The Contractor does have standard project change initiation forms, which can be initiated by either the DHHS or Contractor and encompasses all details of the change including description, specification, time estimates, as well as the required approval procedure. Once this has been approved the Contractor will enter it into our project management application where its status can be easily monitored. It will also appear detailed on the status report.

Escalation Process

The following list illustrates the contact order of ImageTrend staff during escalation of project related tasks:

1. Project Manager, Angie Koch
2. Vice President of Health Data Systems, Michael Patock
3. Sales Manager, Toby Ritt
4. President, Mike McBrady

If there are technical support issues that need escalation during the implementation, please complete steps 1-3 and escalate further if needed:

1. Submit a ticket at: <https://support.imagetrend.com/supportdesk/>
2. Call the Support Team at: 888.469.7789 or 952.469.6132
3. Contact the Project Manager, Angie Koch
4. Contact the Vice President of Health Data Systems, Michael Patock

ACCEPTANCE CRITERIA:

The project shall be considered complete when MDHHS has signed off on the Request for Acceptance Form.

Final Acceptance will occur after the module has been functioning in a production environment without error (*no service, reporting, hardware or software failures*) for a period of 30 days.

Complete testing and acceptance criteria will be mutually detailed during the kick-off meeting. In general, the tasks will be performed by the Contractor with the DHHS responsible for review, modification requests and acceptance. Final acceptance will occur when the agreed upon acceptance criteria have been met, training and documentation have been completed, and the module is deemed to have reached the "Go Live" status.

PROJECT CONTROL AND REPORTS:

A bi-weekly progress report must be submitted to the Agency and DTMB Project Managers throughout the life of this project. This report may be submitted with the billing invoice. Each bi-weekly progress report must contain the following:

1. **Hours:** Indicate the number of hours expended during the past two weeks, and the cumulative total to date for the project. Also state whether the remaining hours are sufficient to complete the project.
2. **Accomplishments:** Indicate what was worked on and what was completed during the current reporting period.
3. **Planned Tasking:** Describe activities to be accomplished during the next reporting period.
4. **Funds:** Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.
5. **Issues:** Indicate major issues/risks/changes, real or perceived, and recommend resolutions.

SPECIFIC DEPARTMENT STANDARDS:

Agency standards, if any, in addition to DTMB standards:
Per Contract 071B4300073 Agreement.

PAYMENT SCHEDULE:

The compensation for services delivered under the Statement of Work will be made in accordance with the EXHIBIT B – Cost, Payment and Compensation.

Payment will be made on a Satisfactory acceptance of each Milestone basis and all invoices must include the purchase order number. DTMB will pay the CONTRACTOR upon receipt of properly completed invoices which shall be submitted to the billing address on the State issued purchase order not more often than monthly. DTMB Contracts area will coordinate obtaining Agency Project Manager and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date, and must be approved by the Agency Project Manager and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense.

Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

EXPENSES:

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:

The designated Agency Project Manager is:

Marvin Helmker, Manager
Department of Health and Human Services
EMS & Trauma Systems Section
Capitol View, 6th Floor
201 Townsend
Lansing, MI 48913
517-241-3024
517-241-9458
HelmkerM1@michigan.gov

The designated DTMB Project Manager is:
Russ Tiedt
DTMB/Customer Service for MDHHS
Application Development
Chandler Plaza/ 1st Floor
300 East Michigan Ave.
Lansing, MI 48933
517-335-3288
(517) 282-4609
TiedtR@michigan.gov

AGENCY RESPONSIBILITIES:

Per Contract 071B4300073 Agreement.

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

Per Contract 071B4300073 Agreement.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:

Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.
No overtime will be permitted.

Exhibit A, Preliminary Progress Plan

The purpose of this document is to provide an overview of milestones and assignment during implementation of the License Management System. Periodic, if not weekly, meetings should be scheduled with your Project Manager, Chris Patera, to ensure timeline objectives are met. If at any time you would like to make changes to this list, please notify Chris Patera or Paul Filla and a review process will ensue from there so we can help accommodate those adjustments. This report is intended to be used as a working, living document that will be shared in order to keep all parties informed of the rollout and additional tasks that are required for completion.



MichiganSOW_WB
S.pdf

EXHIBIT B – Cost, Payment and Compensation

1. Cost Overview for Additional Items

Description	Qty	Price	Less 10% Discount	Extended Price
Legacy Data Migration	100	\$125.00	n/a	\$12,500.00
Payment Gateway Module including Integration Services	1	\$10,000.00	\$1,000.00	\$9,000.00
Payment Gateway Annual Support (4 Years Prepaid)	4	\$2,250.00	n/a	\$9,000.00
Development of License Management Payment Refund Feature	40	\$125.00	n/a/	\$5,000.00
Total				\$35,500.00
Annual Ongoing Fees Year 5 and Thereafter^				\$2,250.00

2. Compensation and Payment

Milestone	Description	Amount Due Upon Completion and State Acceptance of Milestone
Upon Completion and State Acceptance of Legacy Data Migration - <u>Billed at \$125.00 per hour</u>	Legacy Data Migration <i>*Note: The State will only be charged for client determined work efforts that have been signed and accepted by the State. ImageTrend will bill the Legacy Data Migration upon completion and acceptance by the State. The total bill will be based on actual total hours used. Any unused hours will not be invoiced to the State.</i>	\$12,500.00
Upon Completion and State Acceptance of Payment Gateway	Payment Gateway Module <i>*Note: The State will only be charged for the Payment Gateway if agreed to and finally accepted by the State. ImageTrend will bill the Payment Gateway upon completion and acceptance by the State.</i>	\$9,000.00
Upon Completion and State Acceptance of Payment Gateway Annual Support	Payment Gateway Annual Support Fees <i>*Note: Final Acceptance will occur after the module has been functioning in a production environment without error (no service, reporting, hardware or software failures) for a period of 30 days. The State will only be charged for the Payment Gateway if agreed to and accepted by the State. ImageTrend will bill the Payment Gateway upon completion and acceptance by the State after the 30 day acceptance period.</i>	\$9,000.00
Upon Completion and State Acceptance of Development of License Management Payment Refund Feature	Payment License Management Payment Refund Feature <i>*Note: The State will only be charged for the Payment License Management Payment Refund Feature if agreed to and accepted by the State. ImageTrend will bill the Payment License Management Payment Refund Feature upon completion and acceptance by the State.</i>	\$5,000.00
Total Fees	Total Fees (including all Payment Gateway costs)	\$35,500.00
Annual Fees	Year 5 and thereafter Annual Recurring Fees will be invoiced annually on the Go-Live Anniversary*	\$2,250.00

Payment Terms:

- Payment Terms are net 45 days and based upon the Payment Schedule above.
- The recurring Annual Fees for Year 5 and thereafter will be billed annually in advance.

Pricing escalation factors:

- *IMAGETREND may perform price increases of the recurring fees if the State elects to exercise their option for a contract renewal. The State and IMAGETREND will negotiate any increases for Year 5 and thereafter.
- All hosting fees are based upon anticipated usage and include an average of 3 Mb Bandwidth and 30 GB of Storage total. These fees are subject to annual usage audits, which may affect future fees at an increase of \$15/Mb/month for

Bandwidth and \$15/10GB/month for Storage. These price adjustments are subject to negotiations between the parties and will not begin until Year 5 and thereafter.

- c. At least 120 days prior to the beginning of Year 5 IMAGETREND will establish and communicate to CLIENT any of the anticipated increases allowed above.

ID	WBS	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	1	Michigan SOW Project Plan	90 days	Mon 6/1/15	Fri 10/2/15		ImageTrend PM,Michigan PM
2	1.1	Legacy Data Migration	90 days	Mon 6/1/15	Fri 10/2/15		
3	1.1.1	Completion of workbook	1.25 mons	Mon 6/1/15	Fri 7/3/15		Michigan PM
4	1.1.2	Initial Data Migration	25 days	Mon 7/6/15	Fri 8/7/15	3	
5	1.1.2.1	Import Initial Data	2 wks	Mon 7/6/15	Fri 7/17/15		ImageTrend PM
6	1.1.2.2	Review Initial migrated data	2 wks	Mon 7/20/15	Fri 7/31/15	5	Michigan PM
7	1.1.2.3	Approve Initial migrated data	1 wk	Mon 8/3/15	Fri 8/7/15	6	Michigan PM
8	1.1.3	Final Data Migration	20 days	Mon 9/7/15	Fri 10/2/15	7	ImageTrend PM,Michigan PM
9	1.1.3.1	Import Final Data	2 wks	Mon 9/7/15	Fri 9/18/15		ImageTrend PM
10	1.1.3.2	Review Final migrated data	2 wks	Mon 9/21/15	Fri 10/2/15	9	Michigan PM
11	1.1.3.3	Approve Final migrated data	1 wk	Tue 9/22/15	Mon 9/28/15	10	Michigan PM
12	1.2	Payment Gateway	63 days	Wed 7/1/15	Fri 9/25/15		
13	1.2.1	Host Technical Exploration Mtg	12 days	Wed 7/1/15	Thu 7/16/15		ImageTrend PM,Michigan PM
14	1.2.2	Receive Technical access into gateway	25 days	Fri 7/17/15	Thu 8/20/15	13	ImageTrend PM,Michigan PM
15	1.2.3	Configure payment gateway	2 mons	Wed 7/1/15	Tue 8/25/15	14	ImageTrend Dev
16	1.2.4	Test payment gateway	3 wks	Wed 7/29/15	Tue 8/18/15	15	ImageTrend Dev
17	1.2.5	Release payment gateway	33 days	Wed 8/12/15	Fri 9/25/15	16	ImageTrend Dev

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
PROCUREMENT
P.O. BOX 30026, LANSING, MI 48909
OR
525 W. ALLEGAN, LANSING, MI 48933

CHANGE NOTICE NO. 1
to
CONTRACT NO. 071B4300073
between
THE STATE OF MICHIGAN
and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Imagetrend, Inc. 20855 Kensington Blvd Lakeville, MI 55044	Trisha Moline	tmoline@imagetrend.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(952) 469-1589	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR	TBD	TBD	TBD	TBD
BUYER	DTMB	Whitnie Zuker	517-284-7030	zuckerw@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Michigan Emergency Medical Services Information System (MEMSIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
April 1, 2014	September 30, 2019	5, one year	September 30, 2019
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
Net 45	N/A	N/A	N/A
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MiDEAL PARTICIPANTS
<input type="checkbox"/> P-card	<input type="checkbox"/> Direct Voucher (DV)	<input type="checkbox"/> Other	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS:			
N/A			

DESCRIPTION OF CHANGE NOTICE:				
EXTEND CONTRACT EXPIRATION DATE	EXERCISE CONTRACT OPTION YEAR(S)	EXTENSION BEYOND CONTRACT OPTION YEARS	LENGTH OF OPTION/EXTENSION	EXPIRATION DATE AFTER CHANGE
<input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	<input type="checkbox"/>	<input type="checkbox"/>		Sept. 30, 2019
VALUE/COST OF CHANGE NOTICE:			ESTIMATED REVISED AGGREGATE CONTRACT VALUE:	
\$225,300.00			\$946,420.00	

Effective 9/11/2014 this contract is amended to incorporate the attached SOW and increased by \$225,300.00.

Note:

Reserved work is contingent on an approved individual DTMB SOW/Vendor Proposal by the

Department of Technology, Management and Budget (DTMB) Procurement through an executed change notice to the master contract. ImageTrend will not conduct work or charge for this item until it obtains DTMB Procurement approval. The total bill will be based on actual total hours used. Any unused hours will not be invoiced to the State.

This Change Notice is Per Administrative Board Approval on September 11, 2014.

All other terms, conditions, specifications and pricing remain unchanged. Per vendor and agency agreement and DTMB Procurement approval.



**MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK**

Project Title: EMS License Management Implementation	Period of Coverage: 09/15/14 – 09/30/19
Requesting Department: Michigan Department of Community Health (DCH)	Date: 07/17/2014
Agency Project Manager: Marvin Helmker	Phone: 517-241-3024
DTMB Project Manager: George Hamel	Phone: 517-335-3806

Brief Description of Services to be provided:

Purchase order request under contract 071B4300073 - Attachment 6 for Optional Software/Modules components for the web based system to support the Michigan Department of Community Health, EMS Section for time period 09/15/14 - 09/30/19.

BACKGROUND:

DTMB has contract (071B4300073) with ImageTrend, Inc. (“Contractor”) to provide maintenance/support and hosting for Emergency Medical Services (EMS) Michigan Emergency Medical Services Information System (MEMSIS) State Bridge, Visual informatics/Data Mining, and Patient Registry/Trauma Bridge for the Michigan Department of Community Health (MDCH).

The Michigan Department of Community Health, EMS Section, currently licenses 28,000+ EMS personnel, and 820 EMS response agencies. Additionally, the Section is mandated to review and approve EMS education programs, provide oversight of Medical Control Authorities, conduct random audits of licensee continuing education records, and investigate complaints and allegations against EMS personnel. The Section presently uses the L2K system to manage several of its processes. The License Management solution would significantly improve access by our licensees to various required forms, documents, and records. The software would also allow Section personnel to track and monitor progress for each licensee and agency, a process which is presently unavailable.

If not procured, current inefficiencies and services which are not customer-friendly will continue. These include the inability to post agency and vehicle report online, track renewal and expiration dates of licensed vehicles, and electronically track continuing education records for 28,000+ personnel.

PROJECT OBJECTIVE:

The objective of this request is to procure Optional Software/Modules, components that will integrate with the current ImageTrend State Bridge solution to support the Michigan Department of Community Health, EMS Section for the time period of 09/15/14 - 09/30/19.

PRODUCT DESCRIPTION AND OVEVIEW:

See attached Exhibit A for License Management solution description and overview.

Preliminary Progress Plan Document:

See attached Exhibit B, Preliminary Progress Plan Document.

The purpose of this document is to provide an overview of milestones and assignment during implementation of the License Management System. This document is intended to be used as a working, living document that will be shared in order to keep all parties informed of the rollout and additional tasks that are required for completion.

SCOPE OF WORK AND DELIVERABLES:

To implement License Management solution tools to support the EMS web-based system.

1. In Scope

The Contractor will host the License Management application and provide services for the complete and successful implementation of this tool to support the EMS web-based system. The Contractor will provide the functionality required for the State's business operations for the Michigan Department of Community Health, EMS & Trauma Systems Section.

The Contractor must provide a licensing solution designed for processing regulatory licenses and certification, fully web-based, using open architecture and relational database management.

The Contractor will configure the application to incorporate the functionality required to support Michigan program requirements. The system must be able to offer the following types of licensing: Personnel Licensure for First Responder, EMT-B, EMT-Advanced/Intermediate, EMT-P Types, Vehicles Licensure for Ambulances, Services/Agency Licensure for Ground, Air and Private.

In addition to implementing the License Management application, the Contractor will provide:

1. Onsite Training for state program staff
2. Technical knowledge transfer to state staff
3. System and process documentation
4. Testing
5. Project management
6. Support services and system maintenance

2. Work and Deliverables

Contractor shall provide deliverables, services and staff, and otherwise do all things necessary or incidental to provide the functionality required for the State's business operations.

License Management Project Management and Setup

Project management will include 80 hours of project management support for, but not limited to, the implementation process, including the kick off and weekly status meetings as well as software set up and configuration, any integrations, customizations, etc. that need to occur.

Project Planning:

The planning process will begin with a kickoff meeting via teleconference within ten (10) business days after Contract Change Notice execution. The purpose of this meeting is to establish the groundwork for this venture, informing all parties of their roles and responsibilities. The Kickoff meeting will include overall definition of objectives and timelines for the project. Complete testing and acceptance criteria will be mutually detailed during the kick-off meeting. The Contractor will provide to the DCH Project Manager for final acceptance a final project plan and schedule outlining all milestones, tasks, testing and acceptance criteria, roles and responsibilities from both State and Contractor within thirty (30) days after Contract Change Notice execution. Following this, project management and system walkthrough meetings will occur on a weekly basis to complete the Implementation phase.

Hosting:

The Contractor will provide hosting for the web-based License Management solution. All standards and requirements of hosting will be in agreement of the master Contract.

Implementation:

The initial steps of finalization of specifications and acceptance criteria will be accomplished with

Contractor personnel and will be subject to approval by the DCH Project Manager. A task breakdown of a typical Implementation Plan follows:

- Application Review of License Management System in comparison to DCH requirements to include workflows, user interfaces, acceptance criteria and deployment timeframes
- Pilot program definition
- Initial acceptance on the development site to include all agreed upon specification and functions
- Install on the production environment and demonstrate application for pilot program
- Acceptance Testing via pilot program
- Begin Training Plan and schedule ongoing training courses
- System Go-Live
- Ongoing support

Pilot Program:

The basis of the pilot program is the License Management solution. The length for the pilot phase of data collection is thirty days. At the end of this phase a status review and acceptance by the State meeting will be held. The completion of the Pilot Program is a milestone for assessing the overall project success and the form of continuance that will be chosen.

Deployment:

The deployment process for the License Management solution will be established after review of the pilot program.

Contractor personnel will install the License Management solution on Contractor's production servers and the first training courses will be held at a Lansing, MI location and at the days and times agreed upon by DCH. The training courses will be detailed in the training plan (See Training section below). During this phase the system will be accepted by DCH, if deemed acceptable, and will proceed to State acceptance and Go-Live.

Ongoing Support:

Contractor will provide ongoing support for the term of the Contract. This includes continued attention to product performance and maintenance as identified in the master Contract. Contractor's Support Team is available 24/7 at www.imagetrend.com/support as well as Monday through Friday from 7:30 am to 6:00 pm CST at:

Toll Free: 1-888-469-7789
Phone: 952-469-1589

Training:

Contractor will conduct training sessions and deliver training manuals. The Training Curriculum will be reviewed with and accepted by the State and customized to ensure that all courses are designed to address the State's specific needs and will cover all functionalities of the License Management solution. Contractor training for the system to include:

- Five (5) one-day classes in Michigan to train State staff. These classes will be for a maximum of 20 persons. At least two DCH staff in administration, support and maintenance of the system should attend. DCH will provide the training facilities and scheduling;

Contractor will complete onsite Administrator Training, which is designed to get system administrators technical competent with the configuration allowing Contractor to share in best practices in workflow design. Contractor will also complete Technical staff training, which expands on the system administrator training and includes management of the public website design, scheduled tasks, views and PDF generation. This training is aimed at making the State of Michigan self-sufficient on the system.

Contractor will complete Operational (or Internal End User) training, which provides the internal users with a foundation of knowledge to operate the system. Contractor will complete onsite Operational (Internal End User) training, which is designed to get end users competent with the system. ImageTrend will also complete Technical staff training, which expands on the system administrator training and includes management of the public website design, scheduled tasks, views and PDF generation. This training is aimed at making the State of Michigan self-sufficient on the system.

It is recommended that this training be accomplished in a consecutive time frame since the interactive questions and assistance improves the learning process and establishes the communication links for the ongoing system usage. Contractor will hold this training at the location specified by the DCH.

3. Contractor Staff and Roles

The Contractor will provide the following technical staff for implementation, training, monitoring and evaluation reporting.

ImageTrend Inc.

Sales

Lead

Toby Ritt, Sales Manager
tritt@imagetrend.com
952-469-6208

Implementation/Training

Lead

Paul Filla, Implementation Coordinator
pfilla@imagetrend.com
(952) 469-6189

Project Management

Lead

Chris Patera, Project Manager
cpatera@imagetrend.com
(952) 469-6194

Invoicing/Billing

Lead

Tamara Bicknese, Contract & Business Administrator
tbicknese@imagetrend.com
952-469-1589 ext 4005

Development

Lead

Mi Lam, Lead Software Developer
mlam@imagetrend.com
952-469-1589

Integrations

Lead

Sarah Ozanne, Senior Developer
sozanne@imagetrend.com
(952) 469-1589

Statements of Work

Lead

Ryan McCusker, Project Specialist
rmccusker@imagetrend.com

(952) 469-1589

Support

Lead

Alex Faust, Support and Customer Service Lead
afaust@imagetrend.com
1-888-730-3255

Other ImageTrend Contacts

Mike McBrady, President
mmcbrady@imagetrend.com
952-469-6212

Michael Patock, Director of Development
mpatock@imagetrend.com
952-469-6213

Rob Novak, Director of Accounting and Finance
rnovak@imagetrend.com
952-469-6193

Joe Graw, Director Implementation/Support
Implementation Manager
jgraw@imagetrend.com
952-469-6185

Dan Vanorny, Director of Development
mpatock@imagetrend.com
952-469-6229

**4. State Staff and Roles
Information Technology**

Lead

George Hamel
HamelG@michigan.gov
517-335-3806

Operational

Lead

Marvin Helmker
HelmkerM1@michigan.gov
517-241-3024

5. Change Management

Contractor strives to completely assess all requirements and uses past implementation experience to ensure that project change requirements are minimized. Most changes are covered under support or version release policies. However, should a project change(s) be necessary, Contractor will follow the Change Management process of the Master Contract. The Contractor does have standard project change initiation forms, which can be initiated by either the DCH or Contractor and encompasses all details of the change including description, specification, time estimates, as well as the required approval procedure. Once this has been approved the Contractor will enter it into our project management application where its status can be easily monitored. It will also appear detailed on the status report.

6. Escalation Process

The following list illustrates the contact order of ImageTrend staff during escalation of project related

tasks:

1. Implementation Coordinator, Paul Filla
2. Project Manager, Chris Patera
3. Director of Development, Michael Patock
4. Sales Manager, Toby Ritt
5. President, Mike McBrady

If there are technical support issues that need escalation during the implementation, please complete steps 1-3 and escalate further if needed:

1. Submit a ticket at: <https://support.imagetrend.com/supportdesk/>
2. Call the Support Team at: 888.469.7789 or 952.469.6132
3. Contact the Implementation Coordinator, Paul Filla
4. Contact the Project Manager, Chris Patera
5. Contact the Director of Development, Michael Patock

7. Final Acceptance

Final Acceptance will occur after the application has been functioning in a production environment without error (*no service, reporting, hardware or software failures*) for a period of 30 days.

Complete testing and acceptance criteria will be mutually detailed during the kick-off meeting. In general, the tasks will be performed by the Contractor with the DCH responsible for review, modification requests and acceptance. Final acceptance will occur when the agreed upon acceptance criteria have been met, training and documentation have been completed, and the system is deemed to have reached the "Go Live" status.

8. Compensation and Payment

The compensation for services delivered under the Contract will be made in accordance with the deliverables and milestone schedule attached hereto as Exhibit C, Cost, Compensation and Payment.

PROJECT CONTROL AND REPORTS:

A weekly progress report must be submitted to the Agency and DTMB Project Managers throughout the life of this project. This report must be presented to the State prior to invoicing. Each weekly progress report must contain the following:

1. **Hours:** Indicate the number of hours expended during the past two weeks, and the cumulative total to date for the project. Also state whether the remaining hours are sufficient to complete the project.
2. **Accomplishments:** Indicate what was worked on and what was completed during the current reporting period.
3. **Planned Tasking:** Describe activities to be accomplished during the next reporting period.
4. **Funds:** Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.
5. **Issues:** Indicate major issues/risks/changes, real or perceived, and recommend resolutions.

SPECIFIC DEPARTMENT STANDARDS:

Agency standards, if any, in addition to DTMB standards:
Per Contract 071B4300073 Agreement.

PAYMENT SCHEDULE:

Payment will be made on all invoices must include the purchase order number basis. DTMB will pay CONTRACTOR upon receipt of properly completed invoices which shall be submitted to the billing address on

the State issued purchase order not more often than monthly. DTMB Contracts area will coordinate obtaining Agency Project Manager and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date, and must be approved by the Agency Project Manager and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense.

Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

EXPENSES:

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc.

EXHIBIT A – Product Description and Overview

License Management

ImageTrend's **License Management** solution is a highly-configurable, enterprise system that will integrate with the current ImageTrend State Bridge product in place for DCH. It is designed for processing regulatory licenses and certification. The solution incorporates some of ImageTrend's shared platform technologies, including the highly capable Report Writer for generating ad hoc and transactional reports. Each implementation is customized to fit the business rules of the State, making License Management the ideal solution for the State of Michigan's needs.

License Management is Web-based for anytime, anywhere access. The enterprise architecture allows multiple agencies or regulatory boards within a single system for economies of scale and complete reporting. At the same time, each agency has permissions-based access to its own data stores for configuration and reporting. This gives the system just as much flexibility as it has capability.

ImageTrend has developed and hosted statewide data systems since 2001. We understand that the number of users can vary for these systems, and as such the model is not based on seat licenses, yet each user has unique security credentials which can be administered with group permissions.

In addition to the back office administrative functions, License Management has a user-friendly interface for applications and renewals. To secure public trust and transparency, public reporting and license lookup is available through a public Web portal as configured by State.

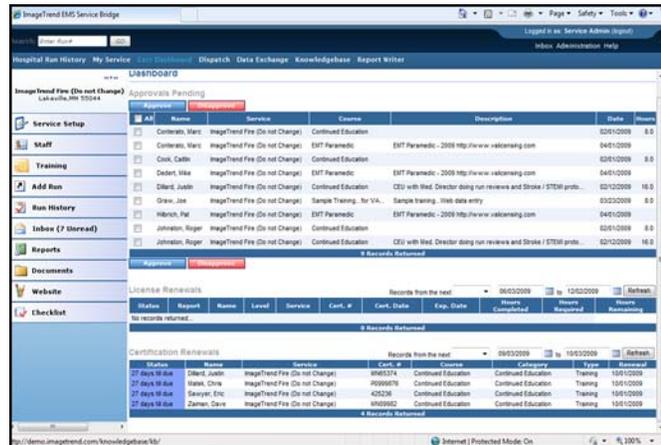
ImageTrend License Management is a complete end-to-end license and certification management solution.

License Management assists agencies in managing and improving the efficiency of end-to-end licensing and records processing, allowing individuals to initiate records, process records through various departments for completion and verification, approve and request copies of

licenses and certificates online. The Web-based solution allows individuals to fill out an application form online. Once an application form is completed, the system administrator view will allow for application review, status tracking and additional processing steps including payment and delivery. Many of the processing steps are either self-service or automated providing both cost and time efficiencies.

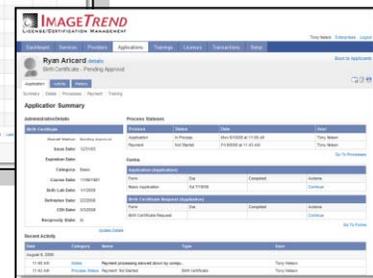
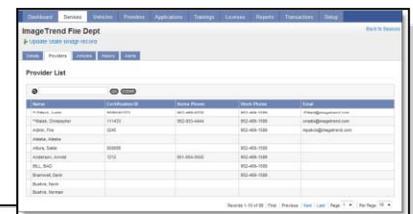
Key Features

- Personnel/Entity/Vehicle Licensing
- Online Payment Processing
- Training Record Collection
- Report Writer
- Automated Workflow
- Content Management Integration for Fully Customizable Public Perspective
- Validate Personnel/Vehicle Licenses
- Universal Login
- Web-based for anytime, anywhere secure access
- Secure access to edit and view information as authorized
- Automated next step processing
- Automated email notifications of tasks and statuses
- Centralized database and processing eliminates redundancies



Workflow

Administrators can establish the specific workflow for each license and certification. The entire process from the application to the payment to the approval can be mapped out by the administrator. Quickly identify your tasks in the easy to view layout, similar to Microsoft Outlook.



Personnel Licensing

Applicants can apply for, renew or request copies for licenses and certificate online. Demographics and other information regarding the applicant's training and examination and status criminal background checks are all collected as required. A license period is set up for easy recording and reporting of renewed licenses. All Personnel Licenses can be audited at any time. The steps involved in the issue of the initial or renewal of any license can be audited at the states discretion. All system transactions are recorded with a

date/time stamp for easy retrieval, and reports can be generated at any time to uncover discrepancies.

Entity Licensing

License Management records each entity (business, shop, organization) license application, including demographics and information regarding the type and level of service, service area, contacts, term of license and inspection date.

Vehicle Licensing

Vehicle information can also be recorded, including model year, manufacturer, vehicle identification number, motor vehicle registration plate, inspection date (if applicable) and vehicle type.

Agency Licensing

The ImageTrend License Management product allows for Agencies/Services to apply for initial licenses and for reinstatement of an expiring licenses. The steps in the application process, supporting documentation required, and necessary business rules and approvals, can be configured by the state after training and implemented in a timeline that fits the state's license terms.

Certification Dashboard

This basic Certification Dashboard allows administrators to track certifications, licenses and coursework for staff members and is included in the base system. If the optional licensure and certification system manager is selected, this will be fully integrated. Staff profiles should include dates for certifications and licenses, which will automatically appear on the Certification Dashboard when renewals are needed. As additional coursework is created, either the administrator or (depending on permissions setup) the staff member can enter information about the hours and types of courses completed towards the certification. The system will automatically update the number of hours completed and needed for the renewal, and allow the administrator to approve or disapprove renewals.

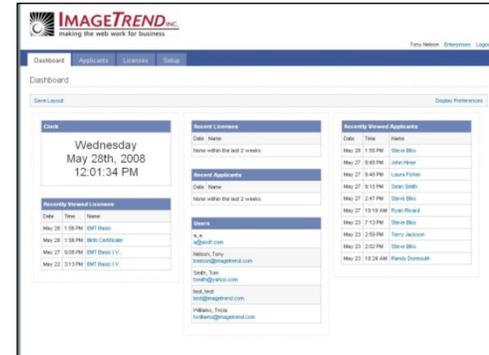
Agency Investigations and Compliance

All Investigations can be recorded and managed by the state through the ImageTrend License Management product. Investigations can be tracked from the individual provider and tied back

the service. Supporting documentation to the investigation can be attached and any additional notes recorded. Alert Flags can be placed on the subjects of the investigation and removed by the system administrator when/if this is applicable.

Virtual License Center Portal

This statewide licensure data management system provides the diversity and expanse required for application usage by multiple agencies throughout the State with virtually unlimited users. The main database server has the complexity and scalability required to collect the magnitude of data presented, as well as provides functional and analytical capabilities for dynamic, up-to-the-minute reporting for use and sharing by government agencies, along with public access where applicable.



User Interfaces

This multi-faceted system allows for many groups to initiate, add, or view information for a certificate, whether that is the initial certificate or a copy. As a self-service online form processing system, considerable time savings will be realized. Copy requests, if they do not require certification, it can be simply downloaded and printed during the initial transaction process. Specific groups will have views to support updating and reviewing information as well as providing authorizations. The multi-tiered access provides data security while ensuring completeness and accuracy. ImageTrend understands that each of the following user groups will have a distinct user interface, which incorporates their specific needs, access rights, workflows and forms.

- Supported functions
 - Profile Management
 - Certificate/License Status and History Lookup
 - Pause-Save-Return-Edit
 - Limited Access
 - Printing
 - Error detection and messages
 - Pre-populated form fields
 - Verification and matching integrations
- Business Process Owner Interface
 - Group Specific Access
 - Limited Edit Rights
 - Group Specific Reporting
 - Group Specific User Management
 - Form Design
 - Form Processing Access

- System Administrator
 - System Wide Access
 - Full Permissions
 - System Wide Reporting
 - System Wide Users and Group Management
 - Resource Management
 - Reporting

Continuing Education Records and Management of Education Programs

ImageTrend License Management allows for the tracking of continuing education records. Available classes can be managed by the state and training instructors can submit applications to conduct additional class or training sessions. The available sessions can be reviewed by personnel who can then contact instructors to be enrolled in the class. Instructors can enroll their students and track which attendees passed/failed the session, as well as recording any applicable exam scores. The state can determine the amount of credits required in each category for a valid license issue.

Management of Medical Control Authorities and Protocols

Services can submit proposed protocols for review and approval by Medical directors and protocols tied to each service can be managed and reported on at the System Administrator level.

Exhibit B, Preliminary Progress Plan

The purpose of this document is to provide an overview of milestones and assignment during implementation of the License Management System. Periodic, if not weekly, meetings should be scheduled with your Project Manager, Chris Patera, to ensure timeline objectives are met. If at any time you would like to make changes to this list, please notify Chris Patera or Paul Filla and a review process will ensue from there so we can help accommodate those adjustments. This report is intended to be used as a working, living document that will be shared in order to keep all parties informed of the rollout and additional tasks that are required for completion.

Title	Status	Date	Ex. Completion Date	Owner	Description & Comments
Determine URL				IT/Client	
Kickoff Meeting				IT/Client	Within 2 weeks of contract signing
Provide existing forms, logos, supporting documents				Client	During or ahead of Kickoff if possible
Provide Process/Workflow related documents				Client	During Kickoff when possible
Provide State/Local regulation documents				Client	During Kickoff when possible
Provide sample legacy data				Client	
Review sample legacy data				IT	
Schedule training dates				IT/Client	Schedule during kickoff meeting
Schedule Payment Portal Merchant Meeting (if any)				Client	Schedule during kickoff meeting

Title	Status	Date	Ex. Completion Date	Owner	Description & Comments
Provide public website branding guidelines (if any)				Client	
Determine ImageTrend State Bridge/Elite to Licensure Integration Parameters (if any)				IT/Client	
Determine additional training requirements				IT/Client	If necessary
Define Pilot Program requirements				IT/Client	If necessary
Review data element manager				IT/Client	
Review System Access Groups				Client	Prior to and during administrator training
Present Project Plan				IT/Client	Within 2 weeks of kickoff meeting
Approve Project Plan				IT/Client	
Setup Site				IT	
Create Administrative Login				IT	
Establish Support Suite Account				Client	
Develop Initial system Access Groups				IT/Client	
Provide Administrator Training				IT	Scheduled
Configure Data Element Manager				Client	
Configure Form(s)				Client	
Configure Correspondence(s)				Client	

Title	Status	Date	Ex. Completion Date	Owner	Description & Comments
Configure Merge Template Email Option(s)				Client	
Configure Triggers				IT/Client	
Configure Public Website				IT/Client	
Configure Alert(s)				Client	
Configure License Duration(s)				Client	
Configure Auto-Number(s)				Client	
Configure Status(es)				Client	
Configure Document Type(s)				Client	
Determine Groups Accessibility				Client	Prior to and during administrator training
Develop Payment Portal Interface				IT	90 days from signing contract
Develop Certification Card/Certificate				IT	60 days from signing of contract
Configure State Bridge to Licensure Integration				IT	
Deploy Pilot Program				IT/Client	If necessary
Evaluate and adjust based on Pilot Program findings				IT/Client	If necessary
Provide additional training				IT	If necessary
Provide Complete Legacy Data in the approved format				Client	

Title	Status	Date	Ex. Completion Date	Owner	Description & Comments
Legacy Data Import				IT	At least 10 days before Go-Live
Go-Live				IT/Client	90 days from kickoff meeting
Develop initial reports through Report Writer				IT/Client	
Acceptance				IT/Client	

EXHIBIT C – Cost, Payment and Compensation

1. Fixed Cost Overview

Description	Qty	Price	Less 10% Discount	Extended Price
License Management License Fee	1	\$125,000.00	\$12,500.00	\$112,500.00
<i>Includes:</i>				
<i>Personnel Licensure for First Responder, EMT-B, EMT-Advanced / Intermediate, EMT-P Types</i>	1	Included	Included	Included
<i>Vehicles Licensure for Ambulances</i>	1	Included	Included	Included
<i>Services/Agency Licensure for Ground, Air and Private</i>	1	Included	Included	Included
Annual Support	1	\$21,600.00	n/a	\$21,600.00
Annual Hosting	1	\$9,000.00	n/a	\$9,000.00
License Management Project Management and Setup	1	\$10,000.00	\$1,000.00	\$9,000.00
Onsite Training Sessions @ \$1,500 per day per trainer	5	\$1,500.00	n/a	\$7,500.00
Year 1 Subtotal				\$159,600.00
Year 2 Support and Hosting				\$32,850.00
Year 3 Support and Hosting				\$32,850.00
Total				\$225,300.00
Annual Ongoing Fees Year 4 and Thereafter^				\$32,850.00

^IMAGETREND may perform price increases of the recurring fees if the State elects to exercise their option for a contract renewal.

2. Reserve Cost Overview

Description	Qty	Price	Less 10% Discount	Extended Price
Legacy Data Migration*	100	\$125.00	n/a	\$12,500.00
Custom Development*	1109	\$125.00	n/a	\$138,625.00

Payment Gateway*	1	\$10,000.00	\$1,000.00	\$9,000.00
Payment Gateway Annual Support	1	\$2,250.00	n/a	\$2,250.00

The extended prices listed above are valid till 9/30/15. There is neither guarantee nor commitment from the State to utilize any or all the costs identified above.

**Note:*

Reserved work is contingent on an approved individual DTMB SOW/Vendor Proposal by the Department of Technology, Management and Budget (DTMB) Procurement through an executed change notice to the master contract. ImageTrend will not conduct work or charge for this item until it obtains DTMB Procurement approval. The total bill will be based on actual total hours used. Any unused hours will not be invoiced to the State.

Payment Terms for individual Statements of Work(s) will be agreed upon based on individual request basis.

3. Compensation and Payment

Milestone	Description	Amount	10% Holdback	Amount Due at Milestone
Contract Signature	100% of One Time License Fee will be invoiced <i>(License Management License Fee, Personnel Licensure for First Responder, EMT-B, EMT-Advanced/Intermediate, EMT-P Types, Vehicles Licensure for Ambulances, Services/Agency Licensure for Ground, Air and Private. Also, included License Management Project Management and Setup)</i>	\$121,500.00	\$12,150.00	\$109,350.00
Upon Completion and State Acceptance of a 30 day Pilot Period (Warranty Period)	100% of Hosting and Support fees for Years 1 will be invoiced	\$30,600.00	\$3,060.00	\$27,540.00
Upon Completion and State Acceptance of Onsite Training 100% of Training fees will be invoiced	100% of Training fees will be invoiced <i>(5 Onsite Training Sessions @ \$1,500 per day per trainer)</i>	\$7,500.00	\$750.00	\$6,750.00

Upon a State Accepted 30 Day Warranty Period After Go-Live	Hold back amount will be invoiced	\$15,960.00	n/a	\$15,960.00
Total Year One	Total Year One Fees	\$159,600.00	n/a	n/a
Annual Fees	Year 2 and thereafter- Annual Recurring Fees will be invoiced annually on the Go-Live Anniversary*	\$32,850.00	n/a	\$32,850.00

Payment Terms:

- a. Payment Terms are net 45 days and based upon the Payment Schedule above.
- b. The recurring Annual Fees for Year 2 and thereafter will be billed annually in advance.

Pricing escalation factors:

- a. IMAGETREND may perform price increases of the recurring fees if the State elects to exercise their option for a contract renewal. The State and IMAGETREND will negotiate any increases for Year 5 and thereafter.
- b. All hosting fees are based upon anticipated usage and include an average of 3 Mb Bandwidth and 30 GB of Storage total. These fees are subject to annual usage audits, which may affect future fees at an increase of \$15/Mb/month for Bandwidth and \$15/10GB/month for Storage. These price adjustments are subject to negotiations between the parties and will not begin until Year 5 and thereafter.
- c. At least 120 days prior to the beginning of Year 5 IMAGETREND will establish and communicate to CLIENT any of the anticipated increases allowed above.

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 530 W. ALLEGAN, LANSING, MI 48933

**NOTICE
 OF
 CONTRACT NO. 071B4300073**
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Imagetrend, Inc. 20855 Kensington Blvd Lakeville, MN 55044	Trisha Moline	tmoline@imagetrend.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(952) 469-1589	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:	TBD	TBD	TBD	TBD
BUYER:	DTMB	Whitnie Zuker	517-284-7030	Zukerw@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Descriptive Contract Title (Not always the same language as provided in MAIN)			
Michigan Emergency Medical Services Information System (MEMSIS)			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
	4/1/2014	9/30/2019	5
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
45			
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MiDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
MISCELLANEOUS INFORMATION:			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:		\$721,120.00	

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation # 0071141114B0001030 (084R4300009). Orders for delivery will be issued directly by the Department of Technology, Management & Budget through the issuance of a Purchase Order Form.

Notice of Contract #: 071B4300073

FOR THE CONTRACTOR:	FOR THE STATE:
Firm Name	Signature
Authorized Agent Signature	Name/Title
Authorized Agent (Print or Type)	Enter Name of Agency
Date	Date

Form No. DTMB-3522 (Rev. 4/2012)
 AUTHORITY: Act 431 of 1984
 COMPLETION: Required
 PENALTY: Contract will not be executed unless form is filed

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 530 W. ALLEGAN, LANSING, MI 48933

CONTRACT NO. 071B4300073
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Imagetrend, Inc. 20855 Kensington Blvd Lakeville, MN 55044	Trisha Moline	tmoline@imagetrend.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(952) 469-1589	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:	TBD	TBD	TBD	TBD
BUYER:	DTMB	Whitnie Zuker	517-284-7030	Zukerw@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Descriptive Contract Title (Not always the same language as provided in MAIN)			
Michigan Emergency Medical Services Information System (MEMSIS)			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
	4/1/2014	9/30/2019	5
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
45			
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MiDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
MISCELLANEOUS INFORMATION:			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION: \$721,120.00			

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation # 0071141114B0001030 (084R4300009). Orders for delivery will be issued directly by the Department of Technology, Management & Budget through the issuance of a Purchase Order Form.

Notice of Contract #: 071B4300073

FOR THE CONTRACTOR:	FOR THE STATE:
Firm Name	Signature
Authorized Agent Signature	Name/Title
Authorized Agent (Print or Type)	Enter Name of Agency
Date	Date

Table of Contents

<u>Article 1 – Statement of Work (SOW)</u>	30
<u>1.000 Project Identification</u>	30
<u>1.001 Project Request</u>	30
<u>1.002 Background</u>	30
<u>1.100 Scope of Work and Deliverables</u>	30
<u>1.101 In Scope</u>	30
<u>1.102 Out Of Scope</u>	31
<u>1.103 Environment</u>	31
<u>1.104 Work And Deliverable</u>	32
<u>1.200 Roles and Responsibilities</u>	39
<u>1.201 Contractor Staff, Roles, And Responsibilities</u>	39
<u>1.202 State Staff, Roles, And Responsibilities</u>	40
<u>1.300 Project Plan</u>	41
<u>1.301 Project Plan Management</u>	41
<u>1.600 Compensation and Payment</u>	45
<u>1.601 Compensation And Payment</u>	45
<u>Article 2, Terms and Conditions</u>	47
<u>2.000 Contract Structure and Term</u>	47
<u>2.001 Contract Term</u>	47
<u>2.002 Options to Renew</u>	47
<u>2.003 Legal Effect</u>	47
<u>2.004 Attachments & Exhibits</u>	47
<u>2.005 Ordering</u>	47
<u>2.006 Order of Precedence</u>	47
<u>2.007 Headings</u>	48
<u>2.008 Form, Function & Utility</u>	48
<u>2.009 Reformation and Severability</u>	48
<u>2.010 Consents and Approvals</u>	48
<u>2.011 No Waiver of Default</u>	48
<u>2.012 Survival</u>	48
<u>2.020 Contract Administration</u>	48
<u>2.021 Issuing Office</u>	48
<u>2.022 Contract Compliance Inspector</u>	49
<u>2.023 Project Manager</u>	49
<u>2.024 Change Requests</u>	49
<u>2.025 Notices</u>	50
<u>2.026 Binding Commitments</u>	50
<u>2.027 Relationship of the Parties</u>	51
<u>2.028 Covenant of Good Faith</u>	51
<u>2.029 Assignments</u>	51
<u>2.030 General Provisions</u>	51
<u>2.031 Administrative Fee and Reporting</u>	51
<u>2.032 Media Releases</u>	52
<u>2.033 Contract Distribution</u>	52
<u>2.034 Permits</u>	52
<u>2.035 Website Incorporation</u>	52
<u>2.036 Future Bidding Preclusion</u>	52
<u>2.037 Freedom of Information</u>	52
<u>2.038 Disaster Recovery</u>	52
<u>2.040 Financial Provisions</u>	52
<u>2.041 Fixed Prices for Services/Deliverables</u>	52
<u>2.042 Adjustments for Reductions in Scope of Services/Deliverables</u>	53
<u>2.043 Services/Deliverables Covered</u>	53
<u>2.044 Invoicing and Payment – In General</u>	53

2.045	Pro-ration	54
2.046	Antitrust Assignment	54
2.047	Final Payment	54
2.048	Electronic Payment Requirement	54
2.050	Taxes	54
2.051	Employment Taxes	54
2.052	Sales and Use Taxes	54
2.060	Contract Management	55
2.061	Contractor Personnel Qualifications	55
2.062	Contractor Key Personnel	55
2.063	Re-assignment of Personnel at the State's Request	55
2.064	Contractor Personnel Location	56
2.065	Contractor Identification	56
2.066	Cooperation with Third Parties	56
2.067	Contract Management Responsibilities	56
2.068	Contractor Return of State Equipment/Resources	56
2.070	Subcontracting by Contractor	56
2.071	Contractor full Responsibility	56
2.072	State Consent to delegation	57
2.073	Subcontractor bound to Contract	57
2.074	Flow Down	57
2.075	Competitive Selection	57
2.080	State Responsibilities	57
2.081	Equipment	57
2.082	Facilities	57
2.090	Security	58
2.091	Background Checks	58
2.100	Confidentiality	58
2.101	Confidentiality	58
2.102	Protection and Destruction of Confidential Information	58
2.103	PCI DATA Security Standard	59
2.104	Exclusions	59
2.105	No Implied Rights	59
2.106	Security Breach Notification	59
2.107	Respective Obligations	60
2.110	Records and Inspections	60
2.111	Inspection of Work Performed	60
2.112	Retention of Records	60
2.113	Examination of Records	60
2.114	Audit Resolution	60
2.115	Errors	60
2.120	Warranties	61
2.121	Warranties and Representations	61
2.122	Warranty of Merchantability	62
2.123	Warranty of Fitness for a Particular Purpose	62
2.124	Warranty of Title	62
2.125	Equipment Warranty	62
2.126	Equipment to be New	63
2.127	Prohibited Products	63
2.128	Consequences for Breach	63
2.130	Insurance	63
2.13.1	Liability Insurance	63
2.13.2	Subcontractor Insurance Coverage	65
2.13.3	Certificates of Insurance	65
2.140	Indemnification	66
2.141	General Indemnification	66
2.142	Code Indemnification	66
2.143	Employee Indemnification	66
2.144	Patent/Copyright Infringement Indemnification	66

2.145	Continuation of Indemnification Obligations	66
2.146	Indemnification Procedures	67
2.150	Termination/Cancellation	67
2.151	Notice and Right to Cure	67
2.152	Termination for Cause	67
2.153	Termination for Convenience	68
2.154	Termination for Non-Appropriation	68
2.155	Termination for Criminal Conviction	69
2.156	Termination for Approvals Rescinded	69
2.157	Rights and Obligations upon Termination	69
2.158	Reservation of Rights	69
2.160	Termination by Contractor	69
2.161	Termination by Contractor	69
2.170	Transition Responsibilities	70
2.171	Contractor Transition Responsibilities	70
2.172	Contractor Personnel Transition	70
2.173	Contractor Information Transition	70
2.174	Contractor Software Transition	70
2.175	Transition Payments	70
2.176	State Transition Responsibilities	70
2.180	Stop Work	71
2.181	Stop Work Orders	71
2.182	Cancellation or Expiration of Stop Work Order	71
2.183	Allowance of Contractor Costs	71
2.190	Dispute Resolution	71
2.191	In General	71
2.192	Informal Dispute Resolution	71
2.193	Injunctive Relief	72
2.194	Continued Performance	72
2.200	Federal and State Contract Requirements	72
2.201	Nondiscrimination	72
2.202	Unfair Labor Practices	72
2.203	Workplace Safety and Discriminatory Harassment	73
2.204	Prevailing Wage	73
2.210	Governing Law	73
2.211	Governing Law	73
2.212	Compliance with Laws	73
2.213	Jurisdiction	73
2.220	Limitation of Liability	74
2.221	Limitation of Liability	74
2.230	Disclosure Responsibilities	74
2.231	Disclosure of Litigation	74
2.232	Call Center Disclosure	74
2.233	Bankruptcy	75
2.240	Performance	75
2.241	Time of Performance	75
2.242	Service Level Agreement (SLA)	75
2.243	Liquidated Damages	76
2.244	Excusable Failure	76
2.250	Approval of Deliverables	77
2.251	Delivery of Deliverables	77
2.252	Contractor System Testing	77
2.253	Approval of Deliverables, In General	78
2.254	Process for Approval of Written Deliverables	79
2.255	Process for Approval of Custom Software Deliverables	79
2.256	Final Acceptance	80
2.260	Ownership	80
2.261	Ownership of Work Product by State	80

2.262	Vesting of Rights	80
2.263	Rights in Data	80
2.264	Ownership of Materials	81
2.270	State Standards	81
2.271	Existing Technology Standards	81
2.272	Acceptable Use Policy	81
2.273	Systems Changes	81
2.274	Electronic Receipt Processing Standard	81
2.280	Extended Purchasing Program	81
2.281	Extended Purchasing Program	81
2.290	Environmental Provision	82
2.291	Environmental Provision	82
2.300	Deliverables	83
2.301	Software	83
2.302	Hardware	83
2.310	Software Warranties	83
2.311	Performance Warranty	83
2.312	No Surreptitious Code Warranty	83
2.313	Calendar Warranty	84
2.314	Third-party Software Warranty	84
2.315	Physical Media Warranty	84
2.320	Software Licensing	85
2.321	Cross-License, Deliverables Only, License to Contractor	85
2.322	Cross-License, Deliverables and Derivative Work, License to Contractor	85
2.323	License Back to the State	85
2.324	License Retained by Contractor	85
2.325	Pre-existing Materials for Custom Software Deliverables	85
2.330	Source Code Escrow	86
2.331	Definition	86
2.332	Delivery of Source Code into Escrow	86
2.333	Delivery of New Source Code into Escrow	86
2.334	Verification	86
2.335	Escrow Fees	86
2.336	Release Events	86
2.337	Release Event Procedures	86
2.338	License	87
2.339	Derivative Works	87
	Glossary	88
	Attachment 1 – Service Level Agreement	90
	Attachment 2 – Hosting Environment	94
	Attachment 3 – ImageTrend Security and Disaster Recovery Process	99
	Attachment 4 – EDS Data Security Policies and Procedures	104
	Attachment 6 – Cost Tables	132

Article 1 – Statement of Work (SOW)

1.000 Project Identification

1.001 PROJECT REQUEST

The State of Michigan (State), through the Department of Technology, Management & Budget (DTMB) in partnership with the Michigan Department of Community Health (MDCH) Emergency Medical Services (EMS) & Trauma Systems Section has issued this Contract for ongoing maintenance, hosting and services for the Michigan Emergency Medical Services Information System (MEMSIS).

The resulting Contract will be for time period of 4/1/2014 through 9/30/2019 with five one-year options to renew.

1.002 BACKGROUND

DCH Emergency Medical Services Mission Statement:

To protect and improve the health and well-being of Michigan citizens who require emergency medical services, through the administration of license requirements for EMS Operations and Vehicles, the oversight of local Medical Control Authorities and the development of regulatory policies and procedures which promote efficient program administration and safe care, treatment and transportation of the sick and injured.

The Emergency Medical Services Section is responsible for licensing over 800 life support agencies and over 3,000 life support vehicles. The Section approves local Medical Control Authorities (a hospital or group of hospitals) that provide community based pre-hospital emergency care oversight. Each county (or group of counties) is required to have such an Authority with the responsibility to establish policies, procedures and protocols focusing specifically on how pre-hospital emergency care will be carried out within their particular geographic area. The section also approves each of the 62 Authority's pre-hospital care policies, procedures and protocols prior to implementation. The Section is responsible to ensure that all life support agencies are in compliance with the communications standards prescribed under the State Medical Communications (MEDCOM) Requirements.

Under part 209 of the Public Health Code, the Michigan Department of Community Health is required to collect Emergency Medical Services data on a statewide basis. The MEMIS is a commercial-off-the-shelf (COTS) NEMSIS compliant application that enables state EMS agencies to securely collect, analyze and report on statewide EMS data. The software allows data to be collected through the use of a web-portal. The portal provides a secure method of collecting pre-hospital data, extracting existing data, and exporting or sharing data with other agencies and applications. Additionally, the software allows ambulance services to satisfy reporting requirements.

1.100 Scope of Work and Deliverables

1.101 IN SCOPE

The Contractor must provide the following services for the complete and successful support, maintenance and hosting of the Michigan Emergency Medical Services Information System (MEMSIS) and associated modules including the functionality required for the State's business operations.

This project consists of the following components:

- A. Maintenance and Support** - Maintenance is defined as repair or replacement services provided after the expiration of the warranty period necessary to identify and repair software malfunctions in order to return the system to its original operating condition. Maintenance also includes an agreement to provide an annual renewable software subscription to include future upgrades (both

major and minor revisions of the application) and ongoing Contractor product support, Help Desk and Technical support.

- B. Hosting**– Contractor hosted solution to include procuring, installing and maintaining application server(s) and other required hardware/software. The solution must include production, development and test/training environments. The development and test hardware/operating system environment will resemble the production environment. The State reserves the option to continue with the Contractor hosted solution or host within the State’s environment for the duration of the contract.
- C. Future Initiatives**– These projects will be determined at time of need and a separate work statement will be developed.

A more complete description of the supplies and/or services sought for this project is provided in Section 1.104, Work and Deliverables.

1.102 OUT OF SCOPE

The State is not seeking a new or replacement system.

1.103 ENVIRONMENT

The links below provide information on the State’s Enterprise information technology (IT) policies, standards and procedures which includes security policy and procedures, IT strategic plan, eMichigan web development and the State Unified Information Technology Environment (SUITE).

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractors are expected to provide proposals that conform to State IT policies and standards. All services and products provided as a result of this Contract must comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response.

Enterprise IT Policies, Standards and Procedures:

<http://www.michigan.gov/dmb/0,1607,7-150-56355-107739--,00.html>

All software and hardware items provided by the Contractor must run on and be compatible with the MDTMB Standard Information Technology Environment. Additionally, the State must be able to maintain software and other items produced as the result of the Contract. Therefore, non-standard development tools may not be used unless approved by MDTMB. The Contractor must request, in writing, approval to use non-standard software development tools, providing justification for the requested change and all costs associated with any change. The MDTMB Project Manager must approve any tools, in writing, before use on any information technology project.

It is recognized that technology changes rapidly. The Contractor may request, in writing, a change in the standard environment, providing justification for the requested change and all costs associated with any change. The State’s Project Manager must approve any changes, in writing, and MDTMB, before work may proceed based on the changed environment.

Enterprise IT Security Policy and Procedures:

http://www.michigan.gov/documents/dmb/1310_183772_7.pdf

http://www.michigan.gov/documents/dmb/1310.02_183775_7.pdf

http://www.michigan.gov/documents/dmb/1325_193160_7.pdf

http://www.michigan.gov/documents/dmb/1335_193161_7.pdf

http://www.michigan.gov/documents/dmb/1340_193162_7.pdf

http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf

IT eMichigan Web Development Standard Tools:

http://www.michigan.gov/documents/som/Look_and_Feel_Standards_302051_7.pdf

The State Unified Information Technology Environment (SUITE):

Includes standards for project management, systems engineering, and associated forms and templates – must be followed: <http://www.michigan.gov/suite>

Current Technical Environment

Contractor must be able to securely maintain, support, enhance and host the MEMSIS using the below licensed software and technical environment to meet the needs of the State.

Current software system components include:

- EMS State Bridge
- Visual Informatics (Data Mining)
- Patient Registry (Trauma Bridge)

Technical Environment includes:

- Database: Microsoft SQL Server 08 R2 or greater
- Development Language: Microsoft .NET
- Development Framework: Microsoft .NET Framework 3.5 or greater
- Web Server: Microsoft IIS version 7.0 or greater
- Application Server: Windows Server 2008 R2 Standard Edition or greater
- Operating System: Microsoft Windows 2008 R2 or greater
- Reporting Tools: ImageTrend State Bridge™ Custom Reporting Module

The Contractor must remain current National EMS Information System (NEMSIS) compliant.

1.104 WORK AND DELIVERABLE

A. Software Maintenance and Support

The Contractor will supply software maintenance and support services that provide systems management as defined below for a flat-fixed annual cost aligned with the State's Fiscal Year. **Further details can be found in Attachment 1 – Service Level Agreement, Attachment 2 – Hosting Environment, Attachment 3 – ImageTrend Security and Disaster Recovery Process and Attachment 4 – EDS Data Security Policies and Procedures:**

- 1. System Maintenance Activities** – Contractor will provide Software maintenance. System Maintenance refers to regular and routine work performed by the Contractor on the MEMSIS. This includes any work required to correct defects in the system operation as required to meet Contract requirements. This also includes any routine file maintenance to update any information required for operation of the system such as data changes, constructing new edits, investigating batch job failures, investigating and correcting application defaults, repairing jobs run incorrectly, repairing problems due to system software failures, repairing problems due to operator or schedule error, rectifying problems due to web page, program, object, class, scripts, control language, or database errors, repairing security problems, repairing and restoring corrupted files, table structures, and databases, rectifying incorrect documentation, and repairing problems due to jobs run with incorrect data.
 - a. The Contractor will perform system maintenance.
 - b. All maintenance will be performed by qualified personnel who are familiar with the system.
 - c. The Contractor will provide backup maintenance resources.
 - d. The Contractor will provide the State access to regular database backup files

- e. The Contractor will provide for escalation of maintenance issues to ensure critical issues are resolved.
- f. The Contractor will provide remote diagnostic capabilities.
- g. The Contractor will provide one point of contact to report system malfunction whether malfunction is due to software or is of unknown origin. The Contractor will then be responsible for providing the appropriate remedy.
- h. The Contractor's annual renewable software subscription must include future upgrades (both major and minor revisions of the application)
- i. The Contractor must coordinate new releases and other changes with the State prior to implementation.
- j. The Contractor must maintain support for the customized medical control authority access.
- k. The Contractor shall offer a live test and training environment alongside of the functioning service. This test and training environment will be loaded with mock data and used by EMS & Trauma Systems Section for training and exercise purposes.
- l. Contractor will provide the following services for the system:
 - i. **Error Correction.** If an error occurs the Contractor shall use commercially reasonable efforts to correct or provide a working solution for the problem. The State will be notified upon discovery of any error and promptly when corrections made.
The State will be provided with information on software problems encountered at other locations, along with the solution to those problems, when such information is relevant to State software
 - ii. **Material Defects.** The Contractor will notify the State of any material errors or defects in the deliverables known, or made known to the Contractor from any source during the Contract term that could cause the production of inaccurate or otherwise materially incorrect, results and shall initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects..
 - iii. **Updates.** All new releases and bug fixes (collectively referred to as "Changes") for any software deliverable developed or published by Contractor and made generally available to its other customers at no additional charge will be provided to the State at no additional charge.

2. Help Desk Support

Contractor must provide a toll free support telephone number 24x365x7 for all users utilizing the MEMSIS. The Contractor must provide on-call staff available 24 hours per day. Internet support and e-mail is also acceptable. The Contractor will provide access to online education materials for all contracted products. The Contractor's Support Team must be available Monday through Friday from 8:00 am to 5:00 pm EST. The response time during business hours are as follows.

Severity Level	Examples of each Severity Level:	Notification Acknowledgement: ImageTrend Return Call to Licensee after initial notification of an Error	Action Expectation: Anticipated Error resolution notification after ImageTrend Return Call to Licensee of Notification Acknowledgement of an error.
Severity 1 – Critical	<ul style="list-style-type: none"> - Complete shutdown or partial shutdown of one or more Software functions - Access to one or more Software functions not available - Major subset of Software application impacted 	Within one (1) hour of initial notification during business hours or via support@imagnetrend.com or Support Desk with critical subject status.	Six hours

Severity 2 – Non-Critical	- Minor subsystem failure -Data entry or access impaired on a limited basis – usually can be delegated to local client contact as a first level or response for resolution – usually user error (i.e. training) or forgotten passwords	Within four (4) hours of initial notification	24 Business hours
Severity 3 – Non-essential	- System operational with minor issues; suggested enhancements as mutually agreed upon – typically covered in next version release as mutually agreed upon.	Same day or next business day of initial notification	Next Release

3. Adaptive and Preventive Maintenance Activities

- a. Adaptive and preventive maintenance addresses upgrades to the system due to technical changes to system components to keep the system maintainable, including the following services:
 - i. Upgrades or patches of the application server, Windows components, operating system, or other system and application software.
 - ii. Software modifications and upgrades necessary because of expiring third party Contractor support.
 - iii. Hardware, database, or application conversions that do not modify user functionality.
 - iv. One-time loads or reformats of user data.
 - v. Report distribution changes.
- b. The changes should be transparent to the end user. The Contractor will provide Release Notes with all system upgrades/updates.
- c. Adaptive release changes will be performed in a quarterly patch release.
- d. For major upgrades requiring a more significant amount of time to develop, test, and implement, the changes should be completed as part of a development release or a quarterly release. Any major release which may require an upgrade to the server/desktop operating systems or third party software utilized as part of the MEMEIS must be documented and provided to the State three months prior to implementation to ensure all requirements can be obtained.
- e. Application Repair –Contractor must offer patches or fixes to acknowledged issues of the MEMEIS within an acceptable timeframe as mutually agreed to by the State and Contractor.

4. Performance Maintenance Activities – assist State staff in performance maintenance activities to improve the performance of the application.

- a. Performance maintenance includes the following services:
 - ii. Improve the performance, maintainability, or other attributes of an application system.
 - iii. Data table restructuring.
 - iv. Data purges and or archiving to reduce/improve data storage.
 - v. Run time improvements.
 - vi. Replace utilities to reduce run time.
 - vii. Potential problem correction.
 - viii. Data set expansions to avoid space problems.

5. Documentation Update

Documentation (electronic) for scheduled software releases to include changes or enhancements to the existing system at no additional cost to the State. Documentation must include:

- For each software release the Contractor must provide release notes to the State detailing the changes/upgrades that are included in the software release. The release notes must identify reported bug fixes and new functionality added by the Contractor.
 - The Contractor will provide the State electronic access to obtain current and future System Administrator Manual or guide and a User Manual which will cover all functions of the current and future contractor's software that is installed and supports the MEMIS. The Contractor will provide a Word version of the Guides and Manuals which the State can customize to detail the MEMIS as installed and configured for the State. If the State would like the Contractor to provide the customization, they can be provided at an additional fee. The State must have unlimited reproduction rights to the manuals for management purposes.
 - The Contractor will provide updated Systems Administrator manuals and User Manuals for major releases that include new functionality in the MEMIS.
- Security Changes- Any changes to user access or administrator access security will be provided in the release notes.

B. Hosting Requirements

The Contractor will supply hosting services as defined below for a flat-fixed annual cost aligned with the State's Fiscal Year.

- i. The Contractor will provide the following for hosting solution during the Contract period:
 - a. Software - Apply hot-fixes and service packs as needed to address anomalies and security concerns. Software support applies to third party software including operating system, back ups, antivirus software, and any application software as related to the hosting services and provided by the Contractor.
 - b. Hardware - Apply Firmware and Bios updates as needed to address anomalies and security concerns. Updates are provided by the hardware Contractor and must be tested internally prior to install.
 - c. Server - Standard hardware and software maintenance as listed above to ensure reliability and optimal performance. This maintenance will occur weekly, monthly and quarterly depending on tasks.
 - d. Firewall - Must be deployed using current industry best practice model. Logs are to be monitored and maintained to ensure reliability and security.
 - e. Anti-Viral – Must provide a reliable industry-standard anti-virus system. Virus definition file maintenance and updates must be done daily to ensure complete virus protection. System must have weekly proactive scans during off peak periods.
 - f. Power Systems and Infrastructure – The facility must meet or exceed the Uptime Institute Tier 3 Data Facility standards. (<http://www.uptimeinstitute.org/>) Primary infrastructure systems must be monitored and redundant, with battery and generator backup power. Circuit load must be checked regularly to ensure reliable power to systems.
 - g. Internet Connectivity - Must be redundant connections with burstable bandwidth support. The connectivity must automatically adjust to handle increased load during an alert.
 - h. Telephone Lines - Service must be maintained and operational tested at regular intervals.
 - i. Encryption & Server Certificates - Must be registered and installed on all web servers. All web traffic transferred from MEMIS to the public internet must be encrypted.
 - j. Domain Names – Must be registered for both the primary and alternate sites. Domain Name Services for all public facing web servers and all internal systems must be maintained and redundant.
 - k. Systems & Data Backup - Must occur nightly. Data must be transferred to tape or other portable media, removed from the data center, and stored at a secure site.
 - l. Systems Failover – Failover to an alternate site is to be available at all times with little or no notice. In order to maintain uptime, critical services must be transferred in the event of a prolonged outage at the primary site. The alternate site must be located geographically separated from the primary site.

- m. Server Computers – Increased hardware capacity may be needed to deal with system expansion and performance needs. The site infrastructure hosting the systems must have the capacity to add additional servers and meet power needs.
- n. Infrastructure Hardware - Should be added as needed to deal with system expansion and performance needs. The site infrastructure hosting the systems must have the capacity to add additional equipment and meet power needs.
- o. Power Systems as Needed - The site infrastructure hosting the systems must have the capacity to add additional power to meet growing needs.
- p. The MEMIS must be fully available 99.9% of the time during normal business hours of 8AM to 5PM EST on business days and also available on-call during non-business hours to support the hosted infrastructure as well as application software.
- q. Performance and Capacity Management
 - Monitor, collect, and analyze Server utilization data for CPU, memory, and disk space;
 - Compile configuration data and usage patterns;
 - Monitor Server performance;
 - Establish thresholds and exception reporting procedures;
 - Perform tuning based on available performance data;
 - Review Server capacity trends;
 - With the State's assistance, establish a schedule for Contractor's performance of Server maintenance (for example, virus and malicious software detection, backup, disk space cleanup) and for implementing modifications and enhancements to the Web Hosting Environment so as to minimally impact availability of the Web Hosting Environment;
 - Fire detection and suppression a system for early detection of fires and suppression in a manner that does not damage state equipment
 - Air conditioning monitored facilities to control for temperature and humidity
 - Facility monitoring for electrical and mechanical failures, fire detection, and leak detection
 - Support services including system and network monitoring of backbone routers, WAN interfaces, routers, switches, and servers
 - Network problem detection, tracking, and resolution process
- r. Security Management
 - Define access controls for the Web Hosting Environment;
 - Monitor the Web Hosting Environment for unauthorized access;
 - Notify the State in accordance with the security procedures specified in the Contractor's Security Guidelines if the Contractor detects a security violation;
 - Follow the procedures specified in the Contractor Security Guidelines for logging, alarming and reporting of security violations;
 - Provide and maintain virus and malicious software avoidance, detection, and elimination software for Servers;
 - Conduct periodic security reviews;
 - Validate the correct use of logical control features such as time-out password screens and password and logon administration;
 - Physical security of the hosting location 24/7 and 365 day (monitored)
 - Controlled access to facilities during business, including logged access by time and date
 - Report access rights for State approval
 - State requires access to regular database backup files
- s. Storage Management Services
 - Maintain and implement database backup and restore processes and procedures to attempt to restore Servers following outages or corruption;
 - Conduct routine backup and restore procedures so as not to adversely impact scheduled operations, including regular backups from disk to tape for the Servers during nightly backup windows;
 - Assist the State in the restoration of files deleted or corrupted.

- The Web Hosting Environment will provide daily incremental backup of all Servers with the ability to restore to the most recent backup;
 - Backup and restore Content;
- t. Reports
1. Server Availability Reports
 - Outage Summary Report
 - Outage by Server Report
 - i. The start and end time of each outage;
 - ii. The duration of the outage;
 - iii. The IP address experiencing the outage;
 - iv. Reason for the outage, if known;
 - v. Description of the actions required to resolve the outage problem;
 - vi. Total time the Server was unavailable; and
 - vii. Name of the Contractors technical team member responsible for resolving the problem.
 2. Performance and Capacity Reports - graphical summary report contains a line graph and a bar chart showing the percentage of Servers in which utilization of a particular resource (i.e., CPU, memory, disk space) was either red, yellow, or green.
 3. Capacity Summary Report - contains a bar chart and a table showing the percentage of Servers in which utilization of a particular resource (i.e., CPU, memory, and disk space) was either red, yellow, or green as defined above. There is also a bar chart and table that show overall resource utilization. The report shows approximately 24 months of data.

u. Hardware –

The Contractor will meet the following Standards:

- Connection: Minimum uptime: 99.9%.
- System availability: 24x7x365.
- An Uninterruptible Power Supply must protect all servers.
- All servers should have dual network cards for fail-over.
- All servers must be located in a security locked room accessible only by authorized personnel
- All outside connections must pass through an approved State of Michigan Firewall.
- All servers are protected by State of Michigan approved Anti-Virus software.
- All servers must pass a State of Michigan approved vulnerability scan, with remediation in 48 hours.
- All servers have their OS upgraded upon release with ample time allowed for bug fixes.
- The Contractors proposed solution must include the following environments:
 - Development
 - Testing
 - Live Production

The Contractor may propose combining environments; however, the Live Production environment must be physically separate from the other environments.

Redundancy shall be designed into the system to handle failure situations and make system maintenance possible without experiencing downtime. Server redundancy is not required; however backup procedures minimize the chance of data loss in the event of a hardware failure. In the event of a prolonged outage due to hardware failure, other servers are available to temporarily run the application. Contractor may provide additional alternatives that will meet the redundancy requirement and will provide a cost savings to the State.

ii. Hosting & Site Security

Physical system security is paramount. All systems must be housed within a secured facility and kept within a secured cabinet or cage. The facility must track and control all access entering and

exiting the building and server room, as well as having physical security systems and video surveillance.

- a. Location of Work Requirements - The work is to be performed, completed, and managed in (2) geographically separated level (3) secure data centers. The data centers must be located in different geographic regions of the United States e.g. California and Texas.
- b. Security and Confidentiality Requirements
 - i. All sites must be secured from Internet, Intranet or On-Site intrusions or attacks.
 - ii. All equipment must be kept secure from On-Site intrusions or attacks.
 - iii. All data must be secured from Internet, Intranet or On-Site intrusions or attacks.
 - iv. All Internet based data transmission must be encrypted.
- iii. Disaster Recovery

Contractor and the State recognize that the State provides essential services in times of natural or man-made disasters. Therefore, except as so mandated by Federal disaster response requirements, Contractor personnel dedicated to providing Services/Deliverables under this Contract will provide the State with priority service for repair and work around in the event of a natural or manmade disaster.

The Contractor will provide a disaster recovery strategy document and include at minimum:

- The strategy to recover to a known state & resume after a site-loss disaster
- The ability to recover on-line transactions since the last backup in a non-site-loss disaster
- An annual demonstration of the ability to recover full functionality to another site
- Off-site transport of system and database backups

The Contractor must provide a document indicating the strategy to maintain system availability in the event of the loss of one or more system components.

Security – In addition to abiding with the disaster recovery and back up process, the Contractor must abide to the security requirements for all of the IT environments being hosted by the Contractor.

C. Future Initiatives

The Contractor will provide an as-needed reserve bank for future software licenses/modules, development or configuration activities, modifications, product enhancements, or work that does not fall under maintenance support as defined in the Contract. The State is not committed to use any of the reserve bank. The State reserves the right to add more to the reserve bank.

Future initiatives must be dependent upon mutually agreed statement(s) of work between the Contractor and the State of Michigan. Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a statement of work until authorized via a purchase order issued against this Contract.

Software

The State reserves the right to purchase additional software licenses/modules to support the State's MEMIS system operations throughout the term of this contract.

Services

The State reserves the right to purchase technical services to support the State's MEMIS system operations throughout the term of the Contract on an as-needed basis.

This reserve bank may be for future services and/or products to meet new requirements that may result from any or all of the following examples:

- A. New State policy requirements,
- B. New Federal regulations, or
- C. New technology requested by the State.

The reserve bank of hours may be used for:

- A. New Development - Contractor may provide the ability for new development work of the software.
- B. Interoperability Development with Other Applications - Contractor may provide the ability to request integrations or interoperability with other products or services of the software.
- C. System Interface Adjustments & New Interfaces – Contractor may provide the ability to request changes or customizations to the application user interface of the software.

The Contractor must be able to respond with costs and timelines to all requests to modify the MEMIS system to meet future needed functionality. Future enhancements must be dependent upon mutually agreed upon statement(s) of work between the Contractor and the State of Michigan. Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a statement of work until authorized via a purchase order issued against this contract.

Each Statements of Work will include:

1. Background
2. Project Objective
3. Scope of Work
4. Deliverables
5. Acceptance Criteria
6. Project Control and Reports
7. Specific Department Standards
8. Cost/Rate
9. Payment Schedule
10. Project Contacts
11. Agency Responsibilities
12. Location of Where the Work is to be performed
13. Expected Contractor Work Hours and Conditions

1.200 Roles and Responsibilities

1.201 CONTRACTOR STAFF, ROLES, AND RESPONSIBILITIES

A. Contractor Staff

The Contractor will provide sufficient qualified staffing to satisfy the deliverables of this Article 1 Statement of Work. Contractor must provide a list of all subcontractors, including firm name, address, contact person, and a complete description of the work to be contracted. Include descriptive information concerning subcontractor's organization and abilities.

The contractor must replace all employees whose work was found to be unsatisfactory as determined by the DTMB project manager within five (5) business days of notification.

The Contractor will provide, and update when changed, an organizational chart indicating lines of authority for personnel involved in performance of the Contract and relationships of this staff to other programs or functions of the firm. This chart must also show lines of authority to the next senior level of management and indicate who within the firm will have prime responsibility and final authority for the work.

Single Point of Contact (SPOC)

The Contractor will identify a SPOC. The duties of the SPOC shall include, but not be limited to:

- supporting the management of the Contract,
- facilitating dispute resolution, and
- advising the State of performance under the terms and conditions of the Contract.

The State reserves the right to require a change in the current SPOC if the assigned SPOC is not, in the opinion of the State, adequately serving the needs of the State.

Key Personnel

The State reserves the right to designate Key Personnel to be provided by the Contractor, as part of individual SOW's. The State reserves the right to interview all Key Personnel and to approve their assignment.

B. On Site Work Requirements

1. Location of Work

The work is to be performed, completed, and managed at the Vendors location. NO work will be performed offshore.

2. Hours of Operation:

- a. Normal State working hours are 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, with work performed as necessary after those hours to meet project deadlines. No overtime will be authorized or paid.
- b. The State is not obligated to provide State management of assigned work outside of normal State working hours. The State reserves the right to modify the work hours in the best interest of the project.
- c. Contractor shall observe the same standard holidays as State employees. The State does not compensate for holiday pay.

3. Travel:

- a. No travel or expenses will be reimbursed, unless formally agreed upon by the State in advanced. This includes travel costs related to training provided to the State by Contractor.
- b. The State is not responsible for providing the use of vehicles for the Contractor.
- c. The State is not responsible for providing housing accommodations to the Contractor.

4. Additional Security and Background Check Requirements:

Contractor must present certifications evidencing satisfactory Michigan State Police Background checks ICHAT and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

1.202 STATE STAFF, ROLES, AND RESPONSIBILITIES

The State will provide the following resources for the Contractor's on-site use, as determined for a specific engagement, through individual Statements of Work. These may include:

- Work space
- Minimal clerical support
- Desk
- Telephone
- PC workstation
- Printer
- Access to copiers and fax machine
- Other. Specify: deemed necessary by DTMB to perform tasks identified in this Contract.

Note: The State reserves the right to inspect and scan any equipment supplied by the Contractor that will be connected to the State's network.

The Contractor is responsible for the return of all State issued equipment in the same condition as when provided by the State, reasonable wear and tear expected, upon Contractor staff release from the project.

The State project team will consist of DTMB and Agency project managers:

State Program Manager-

MDTMB and DCH will provide a Program Manager who will be responsible for overseeing all services performed under the Contract and coordinating with the. The State's Program Managers will provide the following services:

- Supporting the management of the Contract.
- Resolve project issues in a timely manner
- Review project plan, status, and issues
- Resolve deviations from project plan
- Provide acceptance sign-off
- Utilize change control procedures
- Ensure timely availability of State resources
- Make key implementation decisions, as identified by the Contractor's project manager, within 48-hours of their expected decision date.
- Provide State facilities, as needed
- Coordinate the State resources necessary for the project
- Facilitate coordination between various external Contractors
- Facilitate communication between different State departments/divisions
- Provide acceptance and sign-off of deliverable/milestone
- Review and sign-off of timesheets and invoices
- Resolve project issues
- Escalate outstanding/high priority issues
- Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
- Document and archive all important project decisions
- Arrange, schedule and facilitate State staff attendance at all project meetings.
- Escalate outstanding/high priority issues
- Utilize change control procedures
- Conduct regular and ongoing review of the program to confirm that it meets original objectives and requirements
- Document and archive all important program decisions
- Facilitate communication with State project and operational staff.

Name	Agency/Division	Title
George Hamel	MDTMB	Program Manager
Marvin Helmker	MDCH	EMS Manager

1.300 Project Plan

1.301 PROJECT PLAN MANAGEMENT

Project Plan

Specific project plans requirements may be defined within individual Statements of Work.

Contract Kick-Off Meeting

Upon 14 calendar days from execution of the Contract, the Contractor may be required to attend an orientation meeting to discuss the content and procedures of the Contract. The meeting will be held in

Lansing, Michigan, at a date and time mutually acceptable to the state and the Contractor. The state shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Performance Review Meetings

The State may require the Contractor to attend meetings as needed, to review the Contractor's performance under the Contract. The meetings will be held in Lansing, Michigan or by teleconference, as mutually agreed by the State and the Contractor. The State shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Program Control

1. The Contractor will carry out this program under the direction and control of DTMB. The DTMB project manager will review progress reports and will review and approve payments.
2. The Contractor will manage projects in accordance with the State Unified Information Technology Environment (SUITE) methodology, which includes standards for project management, systems engineering, and associated forms and templates which is available at <http://www.michigan.gov/suite>
 - a. Contractor will use an automated tool for planning, monitoring, and tracking the Contract's progress and the level of effort of any Contractor personnel spent performing Services under the Contract. The tool shall have the capability to produce:
 - i. Staffing tables with names of personnel assigned to Contract tasks.
 - ii. Project plans showing tasks, subtasks, deliverables, and the resources required and allocated to each (including detailed plans for all Services to be performed within the next sixty (60) calendar days, updated semi-monthly).
 - iii. Updates must include actual time spent on each task and a revised estimate to complete.
 - iv. Graphs showing critical events, dependencies and decision points during the course of the Contract.
 - b. Any tool(s) used by Contractor for such purposes must produce information of a type and in a manner and format that will support reporting in compliance with the State standards.
3. The DTMB project manager shall have contact as needed with individual Contract employees for the purpose of reviewing progress and providing necessary guidance in solving problems which arise. The objective of this step is to ensure that the DTMB project manager is promptly informed of issues and risks that confront the Contractor employees throughout the Contract.
4. All project assignments and tasks will be undertaken only upon the prior written authorization of the DTMB project manager. The written authorization will include a definition of tasks, deliverables, estimated hours, fixed unit price per hour for each personnel classification, extended price for each personnel classification, maximum price for the authorization, and authorization expiration date. Hours authorized for each task may not be exceeded without a change order issued by the DTMB project manager. If the Contractor employees identify tasks that they anticipate may exceed the estimated amounts, they should notify the DTMB project manager so that any work stoppage may be avoided.

1.302 REPORTS

Specific reporting requirements will be defined within individual Statements of Work. Reporting formats must be submitted to the State's Project Manager for approval within 10 business days after the execution of the Contract. Once both parties have agreed to the format of the report, it shall become the standard to follow for the duration of the Contract. At minimum the status reports shall include:

- Dates of the week covered (daily breakdown by project)
- Contractor name
- DTMB manager name
- Contract name
- P.O. number
- For each project on which the resource worked during the week:
 - Project name
 - Work authorization number

- Number of hours worked on the project for each business day of the week
- Total number of hours worked on the project during the week
- Total number of hours being billed for the week
- DTMB and/or project manager signature and date
- Contractor signature and date

The status report will include the following items for which the resource has worked:

- Project name
- Milestones/deliverables completed
- Tasks accomplished
- Next steps
- Potential issues/risks

1.400 Project Management

1.401 ISSUE MANAGEMENT

An issue is an identified event that if not addressed may affect schedule, scope, quality, or budget.

The Contractor shall maintain an issue log for issues relating to the provision of services under this Contract. The issue management log must be communicated to the State's Project Manager on an agreed upon schedule, with e-mail notifications and updates. The issue log must be updated and must contain the following minimum elements:

1. Description of issue.
2. Issue identification date.
3. Responsibility for resolving issue.
4. Priority for issue resolution (to be mutually agreed upon by the State and the Contractor).
5. Resources assigned responsibility for resolution.
6. Resolution date.
7. Resolution description.

Once the Contractor or the State has identified an issue, the Contractor shall follow these steps:

1. Immediately communicate the issue in writing to the State's Project Manager.
2. The Contractor will log the issue into an issue tracking system.
3. Identify what needs to be done and resources needed to correct the issue.
4. Receive approval from the State's Project Manager for appropriate action.
5. Keep State's Project Manager and appropriate parties informed on status of issue based on frequency established by the State's Project Manager.
6. At least monthly provide a listing of all issues with their current status, deadlines to correct and actual dates of completion that have occurred to the State's Project Manager.

Issues shall be escalated for resolution from level 1 through level 2, as defined below:

- Level 1 – Project Manager
- Level 2 – Contract Compliance Inspector

1.402 RISK MANAGEMENT

A risk is an unknown circumstance or event that, if it occurs, may have a positive or negative impact on the project.

The Contractor is responsible for establishing a risk management plan and process, including the identification and recording of risk items, prioritization of risks, definition of mitigation strategies, monitoring of risk items, and periodic risk assessment reviews with the State.

A risk management plan format shall be submitted to the SOM for approval within twenty (20) business days after Contract signing. The risk management plan will be developed during the initial planning phase of the project, and be in accordance with the SOM PMM methodology. Once both parties have agreed to the format of the plan, it shall become the standard to follow for the duration of the Contract. The plan must be updated bi-weekly, or as agreed upon.

The Contractor shall provide the tool to track risks. The Contractor will work with the SOM and allow input into the prioritization of risks.

The Contractor is responsible for identification of risks for each phase of the project. Mitigating and/or eliminating assigned risks will be the responsibility of the Contractor. The State will assume the same responsibility for risks assigned to them.

1.403 CHANGE MANAGEMENT

Change management is defined as the process to communicate, assess, monitor, and control all changes to system resources and processes. The State also employs change management in its administration of the Contract.

If a proposed Contract change is approved by the Agency, the Contract Administrator will submit a request for change to the Department of Technology, Management and Budget, Procurement Buyer, who will make recommendations to the Director of DTMB-Procurement regarding ultimate approval/disapproval of change request. If the DTMB Procurement Director agrees with the proposed modification, and all required approvals are obtained (including State Administrative Board), the DTMB-Procurement Buyer will issue an addendum to the Contract, via a Contract Change Notice. **Contractors who provide products or services prior to the issuance of a Contract Change Notice by the DTMB-Procurement risk non-payment for the out-of-scope/pricing products and/or services.**

The Contractor must employ change management procedures to handle such things as “out-of-scope” requests or changing business needs of the State while the migration is underway.

The Contractor will employ the change control methodologies to justify changes in the processing environment, and to ensure those changes will not adversely affect performance or availability.

1.500 Acceptance

1.501 CRITERIA

1. The services will be accepted in accordance with the requirements of the Contract.
2. State will review maintenance requests within a mutually agreed upon timeframe from.
 - a. Approvals will be written and signed by State Project Managers.
 - b. Unacceptable issues will be documented and submitted to the Contractor.
 - c. After issues are resolved or waived, the Contractor will resubmit a revised Maintenance Request for Approval of Services within 10 days.
3. The Contractor will maintain the tools and connectivity installed, in compliance with DTMB standards, to properly support and monitor the application.
4. State will review a Request for Approval of Services within a mutually agreed upon timeframe from completion or implementation.
 - a. Approvals will be written and signed by State Project Managers.
 - b. Unacceptable issues will be documented and submitted to the Contractor.
 - c. After issues are resolved or waived, the Contractor will resubmit a Request for Approval of Services for approval within 30 days of receipt.
5. State will review migrated and configured data within a mutually agreed upon timeframe from completion.
 - a. Approvals will be written and signed by State Project Managers.

- b. Unacceptable issues will be documented and submitted to the Contractor.
 - c. After issues are resolved or waived, the Contractor will resubmit a request for approval within 30 days of receipt.
6. The Contractor has the tools and connectivity installed, in compliance with DTMB standards, to properly support and monitor the application.
 7. Specific acceptance criteria for software enhancements will be included in each Statement of Work.
 8. The following criteria apply to software enhancement deliverables:
 - a. Beta software is not accepted as final deliverable.
 - b. MDTMB will review the software enhancements for acceptance of functionality, usability, installation, performance, security, standards compliance, backup/recovery and operation. Approvals will be written and signed by Agency/MDTMB Project Manager as identified in applicable statement of work. Unacceptable issues will be documented and submitted to the Contractor. After issues are resolved or waived, the Contractor will resubmit software for approval.
 - c. Software enhancements are installed and configured in appropriate environment (e.g. development, test, pre-live, live). Contingency plans and de-installation procedures and software are provided by Contractor and approved by the Agency/MDTMB Project Managers as identified in applicable statement of work.
 - d. Contractor will successfully test software enhancements in the development environment before moving the enhancement to the test and pre-live environments for final software testing by Agency/MDTMB. Approvals will be written and signed by Agency/MDTMB Project Managers.
 - e. Unacceptable issues will be documented and submitted to the Contractor. After issues are resolved or waived, the Contractor will resubmit test software, data and results for approval. Only after successful State testing in the test and pre-live area will the enhancement be implemented in the production environment. This implementation should occur at an agreed upon time during non business hours, such as late evenings or weekends.

1.502 FINAL ACCEPTANCE

Final acceptance criteria for deliverables will be identified in each individual project SOW.

1.600 Compensation and Payment

1.601 COMPENSATION AND PAYMENT

Method of Payment

Annual payment shall be made on a firm-fixed cost basis for Maintenance and Hosting Support that aligns with the State's Fiscal Year dates.

For future deliverables, the State reserves the right to determine whether payment shall be made on a firm fixed-hourly rate basis, or on completion and acceptance of specified deliverables or milestones. The parties agree that the Services/Deliverables to be rendered by Contractor pursuant to the Contract (and any future amendments of it) will be defined and described in detail in a Statement of Work.

Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a Statement of Work until authorized via a purchase order issued against the Contract.

Payments will be paid no more than monthly.

The Contractor will not be paid for any costs attributable to corrections of any errors or omissions that have been determined by the DTMB Project Manager to be caused by the Contractor.

Prices quoted will be firm for the entire length of the Contract. For any options to renew (see Section 2.002), prices may not be increased by more than the previous year's Consumer Price Index (CPI) or 3%, whichever is lower.

The Contractor will be required to submit an Administrative Fee (see Section 2.031) on all payments remitted under the Contract.

Notification of Price Reductions

If Contractor reduces its prices for any of the services during the term of the Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send notice to the State's DTMB Procurement Buyer with the reduced prices within fifteen (15) Business Days of the reduction taking effect.

Travel

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc. Travel time will not be reimbursed.

Issuance of Purchase Orders (PO)

Contractor shall not be obliged or authorized to commence any work orders until authorized via a PO issued against this Contract. Contractor shall perform in accordance with this Contract, including the SOWs and Purchase Orders executed under it.

Invoicing

Contractor will submit properly itemized invoices to

DTMB – Financial Services
Accounts Payable
P.O. Box 30026
Lansing, MI 48909
or
DTMB-Accounts-Payable@michigan.gov

Invoices must provide and itemize:

- Contract number;
- Purchase Order number
- Contractor name, address, phone number, and Federal Tax Identification Number;
- Description of service;
- Date(s) of delivery;
- Cost/Rate;
- Total invoice price; and
- Payment terms, including any available prompt payment discount.

Incorrect or incomplete invoices will be returned to Contractor for correction and reissue.

1.602 HOLDBACK

The State shall have the right to hold back an amount equal to percent 10% of all amounts invoiced by Contractor for specified deliverables for future enhancements. The amounts held back shall be released to Contractor after the State has granted Final Acceptance.

Article 2, Terms and Conditions

2.000 Contract Structure and Term

2.001 CONTRACT TERM

This Contract is for a period beginning April 1st, 2014 through September 30th 2019. All outstanding Purchase Orders must also expire upon the termination for any of the reasons listed in **Section 2.150** of the Contract, unless otherwise extended under the Contract. Absent an early termination for any reason, Purchase Orders issued but not expired, by the end of the Contract's stated term, shall remain in effect for the balance of the fiscal year for which they were issued.

2.002 OPTIONS TO RENEW

This Contract may be renewed in writing by mutual agreement of the parties not less than 30 days before its expiration. The Contract may be renewed for up to five (5) additional one (1) year periods.

2.003 LEGAL EFFECT

Contractor accepts this Contract by signing two copies of the Contract and returning them to the DTMB-Procurement. The Contractor shall not proceed with the performance of the work to be done under the Contract, including the purchase of necessary materials, until both parties have signed the Contract to show acceptance of its terms, and the Contractor receives a contract release/purchase order that authorizes and defines specific performance requirements.

Except as otherwise agreed in writing by the parties, the State shall not be liable for costs incurred by Contractor or payment under this Contract, until Contractor is notified in writing that this Contract or Change Order has been approved by the State Administrative Board (if required), signed by all the parties and a Purchase Order against the Contract has been issued.

2.004 ATTACHMENTS & EXHIBITS

All Attachments and Exhibits affixed to any and all Statement(s) of Work, or appended to or referencing this Contract, are incorporated in their entirety and form part of this Contract.

2.005 ORDERING

The State must issue an approved written Purchase Order, Blanket Purchase Order, Direct Voucher or Procurement Card Order to order any Services/Deliverables under this Contract. All orders are subject to the terms and conditions of this Contract. No additional terms and conditions contained on either a Purchase Order or Blanket Purchase Order apply unless they are specifically contained in that Purchase Order or Blanket Purchase Order's accompanying Statement of Work. Exact quantities to be purchased are unknown; however, the Contractor will be required to furnish all such materials and services as may be ordered during the Contract period. Quantities specified, if any, are estimates based on prior purchases, and the State is not obligated to purchase in these or any other quantities.

2.006 ORDER OF PRECEDENCE

The Contract, including any Statements of Work and Exhibits, to the extent not contrary to the Contract, each of which is incorporated for all purposes, constitutes the entire agreement between the parties with respect to the subject matter and supersedes all prior agreements, whether written or oral, with respect to the subject matter and as additional terms and conditions on the purchase order must apply as limited by **Section 2.005**.

In the event of any inconsistency between the terms of the Contract and a Statement of Work, the terms of the Statement of Work shall take precedence (as to that Statement of Work only), provided, however,

that a Statement of Work may not modify or amend the terms of the Contract. The Contract may be modified or amended only by a formal Contract amendment.

2.007 HEADINGS

Captions and headings used in the Contract are for information and organization purposes. Captions and headings, including inaccurate references, do not, in any way, define or limit the requirements or terms and conditions of the Contract.

2.008 FORM, FUNCTION & UTILITY

If the Contract is for use of more than one State agency and if the Deliverable/Service does not meet the form, function, and utility required by that State agency, that agency may, subject to State purchasing policies, procure the Deliverable/Service from another source.

2.009 REFORMATION AND SEVERABILITY

Each provision of the Contract is severable from all other provisions of the Contract and, if one or more of the provisions of the Contract is declared invalid, the remaining provisions of the Contract remain in full force and effect.

2.010 Consents and Approvals

Except as expressly provided otherwise in the Contract, if either party requires the consent or approval of the other party for the taking of any action under the Contract, the consent or approval must be in writing and must not be unreasonably withheld or delayed.

2.011 NO WAIVER OF DEFAULT

If a party fails to insist upon strict adherence to any term of the Contract then the party has not waived the right to later insist upon strict adherence to that term, or any other term, of the Contract.

2.012 SURVIVAL

Any provisions of the Contract that impose continuing obligations on the parties, including without limitation the parties' respective warranty, indemnity and confidentiality obligations, survive the expiration or termination of the Contract for any reason. Specific references to survival in the Contract are solely for identification purposes and not meant to limit or prevent the survival of any other section

2.020 Contract Administration

2.021 ISSUING OFFICE

This Contract is issued by the Department of Technology, Management & Budget, Procurement, the DTMB Customer Services and the Michigan Department of Transportation (MDOT) (collectively, including all other relevant State of Michigan departments and agencies, the "State"). DTMB-Procurement is the sole point of contact in the State with regard to all procurement and contractual matters relating to the Contract. The DTMB-Procurement Contract Administrator for this Contract is:

Whitnie Zuker
Buyer
Procurement
Department of Technology, Management & Budget
Mason Bldg, 2nd Floor
PO Box 30026
Lansing, MI 48909
zukerw@michigan.gov
517-335-5306

2.022 CONTRACT COMPLIANCE INSPECTOR

The Director of DTMB-Procurement directs the person named below, or his or her designee, to monitor and coordinate the activities for the Contract on a day-to-day basis during its term. **Monitoring Contract activities does not imply the authority to change, modify, clarify, amend, or otherwise alter the prices, terms, conditions and specifications of the Contract. DTMB-Procurement is the only State office authorized to change, modify, amend, alter or clarify the prices, specifications, terms and conditions of this Contract.** The Contract Compliance Inspector for this Contract is:

TBD

2.023 PROJECT MANAGER

The following individual will oversee the project:

Marvin Helmker, EMS Manager
EMS Section
Department of Community Health
Capitol View Building, 6th Floor
Lansing, MI 48913
Helmkerm1@michigan.gov
517-241-3024

2.024 CHANGE REQUESTS

The State reserves the right to request from time to time any changes to the requirements and specifications of the Contract and the work to be performed by the Contractor under the Contract. During the course of ordinary business, it may become necessary for the State to discontinue certain business practices or create Additional Services/Deliverables. At a minimum, to the extent applicable, Contractor shall provide a detailed outline of all work to be done, including tasks necessary to accomplish the Additional Services/Deliverables, timeframes, listing of key personnel assigned, estimated hours for each individual per task, and a complete and detailed cost justification.

If the State requests or directs the Contractor to perform any Services/Deliverables that are outside the scope of the Contractor's responsibilities under the Contract ("New Work"), the Contractor must notify the State promptly before commencing performance of the requested activities it believes are New Work. If the Contractor fails to notify the State before commencing performance of the requested activities, any such activities performed before the Contractor gives notice shall be conclusively considered to be in-scope Services/Deliverables and not New Work.

If the State requests or directs the Contractor to perform any services or provide deliverables that are consistent with and similar to the Services/Deliverables being provided by the Contractor under the Contract, but which the Contractor reasonably and in good faith believes are not included within the Statements of Work, then before performing such Services or providing such Deliverables, the Contractor shall notify the State in writing that it considers the Services or Deliverables to be an Additional Service/Deliverable for which the Contractor should receive additional compensation. If the Contractor does not so notify the State, the Contractor shall have no right to claim thereafter that it is entitled to additional compensation for performing that Service or providing that Deliverable. If the Contractor does so notify the State, then such a Service or Deliverable shall be governed by the Change Request procedure in this Section.

In the event prices or service levels are not acceptable to the State, the Additional Services or New Work shall be subject to competitive bidding based upon the specifications.

(1) Change Request at State Request

If the State requires Contractor to perform New Work, Additional Services or make changes to the Services that would affect the Contract completion schedule or the amount of compensation due

Contractor (a "Change"), the State shall submit a written request for Contractor to furnish a proposal for carrying out the requested Change (a "Change Request").

- (2) Contractor Recommendation for Change Requests:
Contractor shall be entitled to propose a Change to the State, on its own initiative, should Contractor believe the proposed Change would benefit the Contract.
- (3) Upon receipt of a Change Request or on its own initiative, Contractor shall examine the implications of the requested Change on the technical specifications, Contract schedule and price of the Deliverables and Services and shall submit to the State without undue delay a written proposal for carrying out the Change. Contractor's proposal shall include any associated changes in the technical specifications, Contract schedule and price and method of pricing of the Services. If the Change is to be performed on a time and materials basis, the Amendment Labor Rates shall apply to the provision of such Services. If Contractor provides a written proposal and should Contractor be of the opinion that a requested Change is not to be recommended, it shall communicate its opinion to the State but shall nevertheless carry out the Change as specified in the written proposal if the State directs it to do so.
- (4) By giving Contractor written notice within a reasonable time, the State shall be entitled to accept a Contractor proposal for Change, to reject it, or to reach another agreement with Contractor. Should the parties agree on carrying out a Change, a written Contract Change Notice must be prepared and issued under this Contract, describing the Change and its effects on the Services and any affected components of this Contract (a "Contract Change Notice").
- (5) No proposed Change shall be performed until the proposed Change has been specified in a duly executed Contract Change Notice issued by the Department of Technology, Management & Budget, Procurement.
- (6) If the State requests or directs the Contractor to perform any activities that Contractor believes constitute a Change, the Contractor must notify the State that it believes the requested activities are a Change before beginning to work on the requested activities. If the Contractor fails to notify the State before beginning to work on the requested activities, then the Contractor waives any right to assert any claim for additional compensation or time for performing the requested activities. If the Contractor commences performing work outside the scope of this Contract and then ceases performing that work, the Contractor must, at the request of the State, retract any out-of-scope work that would adversely affect the Contract.

2.025 NOTICES

Any notice given to a party under the Contract must be deemed effective, if addressed to the party as addressed below, upon: (i) delivery, if hand delivered; (ii) receipt of a confirmed transmission by facsimile if a copy of the notice is sent by another means specified in this Section; (iii) the third Business Day after being sent by U.S. mail, postage pre-paid, return receipt requested; or (iv) the next Business Day after being sent by a nationally recognized overnight express courier with a reliable tracking system.

State:

State of Michigan
DTMB-Procurement
Attention:
PO Box 30026
530 West Allegan
Lansing, Michigan 48909

Contractor:

Name:
Address:

Either party may change its address where notices are to be sent by giving notice according to this Section.

2.026 BINDING COMMITMENTS

Representatives of Contractor must have the authority to make binding commitments on Contractor's behalf within the bounds set forth in the Contract. Contractor may change the representatives from time to time upon giving written notice.

2.027 RELATIONSHIP OF THE PARTIES

The relationship between the State and Contractor is that of client and independent contractor. No agent, employee, or servant of Contractor or any of its Subcontractors shall be deemed to be an employee, agent or servant of the State for any reason. Contractor shall be solely and entirely responsible for its acts and the acts of its agents, employees, servants and Subcontractors during the performance of the Contract.

2.028 COVENANT OF GOOD FAITH

Each party shall act reasonably and in good faith. Unless stated otherwise in the Contract, the parties shall not unreasonably delay, condition or withhold the giving of any consent, decision or approval that is either requested or reasonably required of them in order for the other party to perform its responsibilities under the Contract.

2.029 ASSIGNMENTS

Neither party may assign the Contract, or assign or delegate any of its duties or obligations under the Contract, to any other party (whether by operation of law or otherwise), without the prior written consent of the other party; provided, however, that the State may assign the Contract to any other State agency, department, division or department without the prior consent of Contractor and Contractor may assign the Contract to an affiliate so long as the affiliate is adequately capitalized and can provide adequate assurances that the affiliate can perform the Contract. The State may withhold consent from proposed assignments, subcontracts, or novations when the transfer of responsibility would operate to decrease the State's likelihood of receiving performance on the Contract or the State's ability to recover damages.

Contractor may not, without the prior written approval of the State, assign its right to receive payments due under the Contract. If the State permits an assignment, the Contractor is not relieved of its responsibility to perform any of its contractual duties and the requirement under the Contract that all payments must be made to one entity continues.

If the Contractor intends to assign the contract or any of the Contractor's rights or duties under the Contract, the Contractor must notify the State in writing at least 90 days before the assignment. The Contractor also must provide the State with adequate information about the assignee within a reasonable amount of time before the assignment for the State to determine whether to approve the assignment.

2.030 General Provisions

2.031 ADMINISTRATIVE FEE AND REPORTING

The Contractor must remit an administrative fee of 1% on all payments remitted to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales.

Itemized purchasing activity reports should be mailed to DTMB-Procurement and the administrative fee payments shall be made by check payable to the State of Michigan and mailed to:

The Department of Technology, Management & Budget
Financial Services – Cashier Unit

Lewis Cass Building
320 South Walnut St.
P.O. Box 30681
Lansing, MI 48909

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each quarter.

2.032 MEDIA RELEASES

News releases (including promotional literature and commercial advertisements) pertaining to the RFP and Contract or project to which it relates shall not be made without prior written State approval, and then only in accordance with the explicit written instructions from the State. No results of the activities associated with the RFP and Contract are to be released without prior written approval of the State and then only to persons designated.

2.033 CONTRACT DISTRIBUTION

DTMB-Procurement retains the sole right of Contract distribution to all State agencies and local units of government unless other arrangements are authorized by DTMB-Procurement.

2.034 PERMITS

Contractor must obtain and pay any associated costs for all required governmental permits, licenses and approvals for the delivery, installation and performance of the Services. The State shall pay for all costs and expenses incurred in obtaining and maintaining any necessary easements or right of way.

2.035 WEBSITE INCORPORATION

The State is not bound by any content on the Contractor's website, even if the Contractor's documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the State has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by an authorized representative of the State.

2.036 FUTURE BIDDING PRECLUSION

Contractor acknowledges that, to the extent this Contract involves the creation, research, investigation or generation of a future RFP, it may be precluded from bidding on the subsequent RFP. The State reserves the right to disqualify any Bidder if the State determines that the Bidder has used its position (whether as an incumbent Contractor, or as a Contractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP.

2.037 FREEDOM OF INFORMATION

All information in any proposal submitted to the State by Contractor and this Contract is subject to the provisions of the Michigan Freedom of Information Act, 1976 Public Act No. 442, as amended, MCL 15.231, et seq (the "FOIA").

2.038 DISASTER RECOVERY

Contractor and the State recognize that the State provides essential services in times of natural or man-made disasters. Therefore, except as so mandated by Federal disaster response requirements, Contractor personnel dedicated to providing Services/Deliverables under this Contract shall provide the State with priority service for repair and work around in the event of a natural or man-made disaster.

2.040 Financial Provisions

2.041 FIXED PRICES FOR SERVICES/DELIVERABLES

Each Statement of Work or Purchase Order issued under this Contract shall specify (or indicate by reference to the appropriate Contract Exhibit) the firm, fixed prices for all Services/Deliverables, and the associated payment milestones and payment amounts. The State may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor shall show verification of measurable progress at the time of requesting progress payments.

2.042 ADJUSTMENTS FOR REDUCTIONS IN SCOPE OF SERVICES/DELIVERABLES

If the scope of the Services/Deliverables under any Statement of Work issued under this Contract is subsequently reduced by the State, the parties shall negotiate an equitable reduction in Contractor's charges under such Statement of Work commensurate with the reduction in scope.

2.043 SERVICES/DELIVERABLES COVERED

The State shall not be obligated to pay any amounts in addition to the charges specified in this Contract for all Services/Deliverables to be provided by Contractor and its Subcontractors, if any, under this Contract.

2.044 INVOICING AND PAYMENT – IN GENERAL

- (a) Each Statement of Work issued under this Contract shall list (or indicate by reference to the appropriate Contract Exhibit) the prices for all Services/Deliverables, equipment and commodities to be provided, and the associated payment milestones and payment amounts.
- (b) Each Contractor invoice shall show details as to charges by Service/Deliverable component and location at a level of detail reasonably necessary to satisfy the State's accounting and charge-back requirements. Invoices for Services performed on a time and materials basis shall show, for each individual, the number of hours of Services performed during the billing period, the billable skill/labor category for such person and the applicable hourly billing rate. Prompt payment by the State is contingent on the Contractor's invoices showing the amount owed by the State minus any holdback amount to be retained by the State in accordance with **Section 1.600**.
- (c) Correct invoices shall be due and payable by the State, in accordance with the State's standard payment procedure as specified in 1984 Public Act No. 279, MCL 17.51 et seq., within 45 days after receipt, provided the State determines that the invoice was properly rendered.
- (d1) All invoices should reflect actual work done. Specific details of invoices and payments shall be agreed upon between the Contract Administrator and the Contractor after the proposed Contract Agreement has been signed and accepted by both the Contractor and the Director of Procurement, Department of Management & Budget. This activity shall occur only upon the specific written direction from DTMB-Procurement.

The specific payment schedule for any Contract(s) entered into, as the State and the Contractor(s) shall mutually agree upon. The schedule should show payment amount and should reflect actual work done by the payment dates, less any penalty cost charges accrued by those dates. As a general policy statements shall be forwarded to the designated representative by the 15th day of the following month.

The Government may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor must show verification of measurable progress at the time of requesting progress payments.

(b) (d2) Contract Payment Schedule

1. Contractor request for performance-based payment.

The Contractor may submit requests for payment of performance-based payments not more frequently than monthly, in a form and manner acceptable to the Contract Administrator. Unless otherwise authorized by the Contract Administrator, all performance-based payments in any period for which payment is being requested shall be included in a single request, appropriately itemized and totaled.

2. Approval and payment of requests.

The Contractor shall not be entitled to payment of a request for performance-based payment prior to successful accomplishment of the event or performance criterion for which payment is requested. The Contract Administrator shall determine whether the event or performance criterion for which payment is requested has been successfully accomplished in accordance with the terms of the contract. The Contract Administrator may, at any time, require the Contractor to substantiate the successful performance of any event or performance criterion, which has been or is represented as being payable.

A payment under this performance-based payment clause is a contract financing payment under the Quick Payment Terms in **Section 1.600** of this Contract.

The approval by the Contract Administrator of a request for performance-based payment does not constitute an acceptance by the Government and does not excuse the Contractor from performance of obligations under this Contract.

2.045 PRO-RATION

To the extent there are Services that are to be paid for on a monthly basis, the cost of such Services shall be pro-rated for any partial month.

2.046 ANTITRUST ASSIGNMENT

The Contractor assigns to the State any claim for overcharges resulting from antitrust violations to the extent that those violations concern materials or services supplied by third parties to the Contractor, toward fulfillment of this Contract.

2.047 FINAL PAYMENT

The making of final payment by the State to Contractor does not constitute a waiver by either party of any rights or other claims as to the other party's continuing obligations under the Contract, nor shall it constitute a waiver of any claims by one party against the other arising from unsettled claims or failure by a party to comply with this Contract, including claims for Services and Deliverables not reasonably known until after acceptance to be defective or substandard. Contractor's acceptance of final payment by the State under this Contract shall constitute a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still unsettled.

2.048 ELECTRONIC PAYMENT REQUIREMENT

Electronic transfer of funds is required for payments on State Contracts. Contractors are required to register with the State electronically at <http://www.cpexpress.state.mi.us>. As stated in Public Act 431 of 1984, all contracts that the State enters into for the purchase of goods and services shall provide that payment shall be made by electronic fund transfer (EFT).

2.050 Taxes

2.051 EMPLOYMENT TAXES

Contractor shall collect and pay all applicable federal, state, and local employment taxes, including the taxes.

2.052 SALES AND USE TAXES

Contractor shall register and remit sales and use taxes on taxable sales of tangible personal property or services delivered into the State. Contractors that lack sufficient presence in Michigan to be required to register and pay tax must do so as a volunteer. This requirement extends to: (1) all members of any controlled group as defined in § 1563(a) of the Internal Revenue Code and applicable regulations of which the company is a member, and (2) all organizations under common control as defined in § 414(c)

of the Internal Revenue Code and applicable regulations of which the company is a member that make sales at retail for delivery into the State are registered with the State for the collection and remittance of sales and use taxes. In applying treasury regulations defining "two or more trades or businesses under common control" the term "organization" means sole proprietorship, a partnership (as defined in § 701(a) (2) of the Internal Revenue Code), a trust, an estate, a corporation, or a limited liability company.

2.060 Contract Management

2.061 CONTRACTOR PERSONNEL QUALIFICATIONS

All persons assigned by Contractor to the performance of Services under this Contract must be employees of Contractor or its majority-owned (directly or indirectly, at any tier) subsidiaries (or a State-approved Subcontractor) and must be fully qualified to perform the work assigned to them. Contractor must include a similar provision in any subcontract entered into with a Subcontractor. For the purposes of this Contract, independent contractors engaged by Contractor solely in a staff augmentation role must be treated by the State as if they were employees of Contractor for this Contract only; however, the State understands that the relationship between Contractor and Subcontractor is an independent contractor relationship.

2.062 CONTRACTOR KEY PERSONNEL

- (a) The Contractor must provide the Contract Compliance Inspector with the names of the Key Personnel.
- (b) Key Personnel must be dedicated as defined in the Statement of Work to the Project for its duration in the applicable Statement of Work with respect to other individuals designated as Key Personnel for that Statement of Work.
- (c) The State shall have the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor shall notify the State of the proposed assignment, shall introduce the individual to the appropriate State representatives, and shall provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State shall provide a written explanation including reasonable detail outlining the reasons for the rejection.
- (d) Contractor must not remove any Key Personnel from their assigned roles on the Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("Unauthorized Removal"). Unauthorized Removals does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation or for cause termination of the Key Personnel's employment. Unauthorized Removals does not include replacing Key Personnel because of promotions or other job movements allowed by Contractor personnel policies or Collective Bargaining Agreement(s) as long as the State receives prior written notice before shadowing occurs and Contractor provides 30 days of shadowing unless parties agree to a different time period. The Contractor with the State must review any Key Personnel replacements, and appropriate transition planning will be established. Any Unauthorized Removal may be considered by the State to be a material breach of the Contract, in respect of which the State may elect to exercise its termination and cancellation rights.
- (e) The Contractor must notify the Contract Compliance Inspector and the Contract Administrator at least 10 business days before redeploying non-Key Personnel, who are dedicated to primarily to the Project, to other projects. If the State does not object to the redeployment by its scheduled date, the Contractor may then redeploy the non-Key Personnel.

2.063 RE-ASSIGNMENT OF PERSONNEL AT THE STATE'S REQUEST

The State reserves the right to require the removal from the Project of Contractor personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request must be based on

legitimate, good faith reasons. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed personnel, the State agrees to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any incident with removed personnel results in delay not reasonably anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Service shall not be counted for a time as agreed to by the parties.

2.064 CONTRACTOR PERSONNEL LOCATION

All staff assigned by Contractor to work on the Contract shall perform their duties either primarily at Contractor's offices and facilities or at State facilities. Without limiting the generality of the foregoing, Key Personnel shall, at a minimum, spend at least the amount of time on-site at State facilities as indicated in the applicable Statement of Work. Subject to availability, selected Contractor personnel may be assigned office space to be shared with State personnel.

2.065 CONTRACTOR IDENTIFICATION

Contractor employees must be clearly identifiable while on State property by wearing a State-issued badge, as required. Contractor employees are required to clearly identify themselves and the company they work for whenever making contact with State personnel by telephone or other means.

2.066 COOPERATION WITH THIRD PARTIES

Contractor agrees to cause its personnel and the personnel of any Subcontractors to cooperate with the State and its agents and other contractors including the State's Quality Assurance personnel. As reasonably requested by the State in writing, the Contractor shall provide to the State's agents and other contractors reasonable access to Contractor's Project personnel, systems and facilities to the extent the access relates to activities specifically associated with this Contract and shall not interfere or jeopardize the safety or operation of the systems or facilities. The State acknowledges that Contractor's time schedule for the Contract is very specific and agrees not to unnecessarily or unreasonably interfere with, delay or otherwise impeded Contractor's performance under this Contract with the requests for access.

2.067 CONTRACT MANAGEMENT RESPONSIBILITIES

Contractor shall be responsible for all acts and omissions of its employees, as well as the acts and omissions of any other personnel furnished by Contractor to perform the Services. Contractor shall have overall responsibility for managing and successfully performing and completing the Services/Deliverables, subject to the overall direction and supervision of the State and with the participation and support of the State as specified in this Contract. Contractor's duties shall include monitoring and reporting the State's performance of its participation and support responsibilities (as well as Contractor's own responsibilities) and providing timely notice to the State in Contractor's reasonable opinion if the State's failure to perform its responsibilities in accordance with the Project Plan is likely to delay the timely achievement of any Contract tasks.

The Contractor shall provide the Services/Deliverables directly or through its affiliates, subsidiaries, subcontractors or resellers. Regardless of the entity providing the Service/Deliverable, the Contractor shall act as a single point of contact coordinating these entities to meet the State's need for Services/Deliverables. Nothing in this Contract, however, shall be construed to authorize or require any party to violate any applicable law or regulation in its performance of this Contract.

2.068 CONTRACTOR RETURN OF STATE EQUIPMENT/RESOURCES

The Contractor shall return to the State any State-furnished equipment, facilities and other resources when no longer required for the Contract in the same condition as when provided by the State, reasonable wear and tear excepted.

2.070 Subcontracting by Contractor

2.071 CONTRACTOR FULL RESPONSIBILITY

Contractor shall have full responsibility for the successful performance and completion of all of the Services and Deliverables. The State shall consider Contractor to be the sole point of contact with regard to all contractual matters under this Contract, including payment of any and all charges for Services and Deliverables.

2.072 STATE CONSENT TO DELEGATION

Contractor shall not delegate any duties under this Contract to a Subcontractor unless the Department of Technology, Management & Budget, Procurement has given written consent to such delegation. The State shall have the right of prior written approval of all Subcontractors and to require Contractor to replace any Subcontractors found, in the reasonable judgment of the State, to be unacceptable. The State's request shall be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request shall be based on legitimate, good faith reasons. Replacement Subcontractor(s) for the removed Subcontractor shall be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed Subcontractor, the State shall agree to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any such incident with a removed Subcontractor results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLA for the affected Work shall not be counted for a time agreed upon by the parties.

2.073 SUBCONTRACTOR BOUND TO CONTRACT

In any subcontracts entered into by Contractor for the performance of the Services, Contractor shall require the Subcontractor, to the extent of the Services to be performed by the Subcontractor, to be bound to Contractor by the terms of this Contract and to assume toward Contractor all of the obligations and responsibilities that Contractor, by this Contract, assumes toward the State. The State reserves the right to receive copies of and review all subcontracts, although Contractor may delete or mask any proprietary information, including pricing, contained in such contracts before providing them to the State. The management of any Subcontractor shall be the responsibility of Contractor, and Contractor shall remain responsible for the performance of its Subcontractors to the same extent as if Contractor had not subcontracted such performance. Contractor shall make all payments to Subcontractors or suppliers of Contractor. Except as otherwise agreed in writing by the State and Contractor, the State shall not be obligated to direct payments for the Services other than to Contractor. The State's written approval of any Subcontractor engaged by Contractor to perform any obligation under this Contract shall not relieve Contractor of any obligations or performance required under this Contract. A list of the Subcontractors, if any, approved by the State as of the execution of this Contract, together with a copy of the applicable subcontract is attached.

2.074 FLOW DOWN

Except where specifically approved in writing by the State on a case-by-case basis, Contractor shall flow down the obligations in **Sections 2.031, 2.060, 2.100, 2.110, 2.120, 2.130, and 2.200** in all of its agreements with any Subcontractors.

2.075 COMPETITIVE SELECTION

The Contractor shall select subcontractors (including suppliers) on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the Contract.

2.080 State Responsibilities

2.081 EQUIPMENT

The State shall provide only the equipment and resources identified in the Statement of Work and other Contract Exhibits.

2.082 FACILITIES

The State must designate space as long as it is available and as provided in the Statement of Work, to house the Contractor's personnel whom the parties agree will perform the Services/Deliverables at State facilities (collectively, the "State Facilities"). The Contractor shall have reasonable access to, and unless agreed otherwise by the parties in writing must observe and comply with all rules and regulations relating to each of the State Facilities (including hours of operation) used by the Contractor in the course of providing the Services. Contractor agrees that it shall not, without the prior written consent of the State, use any State Facilities or access any State information systems provided for the Contractor's use, or to which the Contractor otherwise gains access in the course of performing the Services, for any purpose other than providing the Services to the State.

2.090 Security

2.091 BACKGROUND CHECKS

On a case-by-case basis, the State may investigate the Contractor's personnel before they may have access to State facilities and systems. The scope of the background check is at the discretion of the State and the results shall be used to determine Contractor personnel eligibility for working within State facilities and systems. The investigations shall include Michigan State Police Background checks (ICHAT) and may include the National Crime Information Center (NCIC) Finger Prints. Proposed Contractor personnel may be required to complete and submit an RI-8 Fingerprint Card for the NCIC Finger Print Check. Any request for background checks shall be initiated by the State and shall be reasonably related to the type of work requested.

2.100 Confidentiality

2.101 CONFIDENTIALITY

Contractor and the State each acknowledge that the other possesses and shall continue to possess confidential information that has been developed or received by it. As used in this Section, "Confidential Information" of Contractor must mean all non-public proprietary information of Contractor (other than Confidential Information of the State as defined below), which is marked confidential, restricted, proprietary, or with a similar designation. "Confidential Information" of the State must mean any information which is retained in confidence by the State (or otherwise required to be held in confidence by the State under applicable federal, state and local laws and regulations) or which, in the case of tangible materials provided to Contractor by the State under its performance under this Contract, is marked as confidential, proprietary or with a similar designation by the State. "Confidential Information" excludes any information (including this Contract) that is publicly available under the Michigan FOIA.

2.102 PROTECTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION

The State and Contractor shall each use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication or dissemination of its own confidential information of like character, but in no event less than reasonable care. Neither Contractor nor the State shall (i) make any use of the Confidential Information of the other except as contemplated by this Contract, (ii) acquire any right in or assert any lien against the Confidential Information of the other, or (iii) if requested to do so, refuse for any reason to promptly return the other party's Confidential Information to the other party. Each party shall limit disclosure of the other party's Confidential Information to employees and Subcontractors who must have access to fulfill the purposes of this Contract. Disclosure to, and use by, a Subcontractor is permissible where (A) use of a Subcontractor is authorized under this Contract, (B) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Subcontractor's scope of responsibility, and (C) Contractor obligates the Subcontractor in a written Contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor and of any Subcontractor having access or continued access to the State's Confidential Information may be required to execute an acknowledgment that the employee has been advised of Contractor's and the Subcontractor's obligations

under this Section and of the employee's obligation to Contractor or Subcontractor, as the case may be, to protect the Confidential Information from unauthorized use or disclosure.

Promptly upon termination or cancellation of the Contract for any reason, Contractor must certify to the State that Contractor has destroyed all State Confidential Information.

2.103 PCI DATA SECURITY STANDARD

(a) Contractors that process, transmit or store credit/debit cardholder data, must adhere to the Payment Card Industry (PCI) Data Security Standards. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

(b) The Contractor must notify the CCI (within 72 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the Visa, MasterCard, Discover and state Acquirer representative(s), and/or a PCI approved third party to conduct a thorough security review. The Contractor must make the forensic report available within two weeks of completion. The review must validate compliance with the current PCI Data Security Standards for protecting cardholder data.

(c) The Contractor must properly dispose of cardholder data, in compliance with DTMB policy, when it is no longer needed. The Contractor must continue to treat cardholder data as confidential upon contract termination.

(d) The Contractor must provide the CCI with an annual Attestation of Compliance (AOC) or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standards. The Contractor must notify the CCI of all failures to comply with the PCI Data Security Standard.

2.104 EXCLUSIONS

Notwithstanding the foregoing, the provisions in this Section shall not apply to any particular information which the State or Contractor can demonstrate (i) was, at the time of disclosure to it, in the public domain; (ii) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party; (iii) was in the possession of the receiving party at the time of disclosure to it without an obligation of confidentiality; (iv) was received after disclosure to it from a third party who had a lawful right to disclose the information to it without any obligation to restrict its further disclosure; or (v) was independently developed by the receiving party without reference to Confidential Information of the furnishing party. Further, the provisions of this Section shall not apply to any particular Confidential Information to the extent the receiving party is required by law to disclose the Confidential Information, provided that the receiving party (i) promptly provides the furnishing party with notice of the legal request, and (ii) assists the furnishing party in resisting or limiting the scope of the disclosure as reasonably requested by the furnishing party.

2.105 NO IMPLIED RIGHTS

Nothing contained in this Section must be construed as obligating a party to disclose any particular Confidential Information to the other party, or as granting to or conferring on a party, expressly or impliedly, any right or license to the Confidential Information of the other party.

2.106 SECURITY BREACH NOTIFICATION

If the Contractor breaches this Section, the Contractor must (i) promptly cure any deficiencies and (ii) comply with any applicable federal and state laws and regulations pertaining to unauthorized disclosures. Contractor and the State shall cooperate to mitigate, to the extent practicable, the effects of any breach, intrusion, or unauthorized use or disclosure. Contractor must report to the State in writing any use or disclosure of Confidential Information, whether suspected or actual, other than as provided for by the Contract within 72 hours of becoming aware of the use or disclosure or the shorter time period as is reasonable under the circumstances.

2.107 RESPECTIVE OBLIGATIONS

The parties' respective obligations under this Section must survive the termination or expiration of this Contract for any reason.

2.110 Records and Inspections

2.111 INSPECTION OF WORK PERFORMED

The State's authorized representatives, at reasonable times and with 10 days prior notice, have the right to enter the Contractor's premises or any other places where work is being performed in relation to this Contract. The representatives may inspect, monitor, or evaluate the work being performed, to the extent the access will not reasonably interfere with or jeopardize the safety or operation of Contractor's systems or facilities. The Contractor must provide reasonable assistance for the State's representatives during inspections.

2.112 RETENTION OF RECORDS

(a) The Contractor must retain all financial and accounting records related to this Contract for a period of 7 years after the Contractor performs any work under this Contract (Audit Period).

(b) If an audit, litigation, or other action involving the Contractor's records is initiated before the end of the Audit Period, the Contractor must retain the records until all issues arising out of the audit, litigation, or other action are resolved or until the end of the Audit Period, whichever is later.

2.113 EXAMINATION OF RECORDS

(a) The State, upon 10 days notice to the Contractor, may examine and copy any of the Contractor's records that relate to this Contract any time during the Audit Period. The State does not have the right to review any information deemed confidential by the Contractor if access would require the information to become publicly available. This requirement also applies to the records of any parent, affiliate, or subsidiary organization of the Contractor, or any Subcontractor that performs services in connection with this Contract

(b) In addition to the rights conferred upon the State in paragraph (a) of this section and in accordance with MCL 18.1470, DTMB or its designee may audit the Contractor to verify compliance with the Contract. The financial and accounting records associated with the Contract shall be made available to DTMB or its designee and the auditor general, upon request, during the term of the Contract and any extension of the Contract and for 3 years after the later of the expiration date or final payment under the Contract.

2.114 AUDIT RESOLUTION

If necessary, the Contractor and the State will meet to review any audit report promptly after its issuance. The Contractor must respond to each report in writing within 30 days after receiving the report, unless the report specifies a shorter response time. The Contractor and the State must develop, agree upon, and monitor an action plan to promptly address and resolve any deficiencies, concerns, or recommendations in the report.

2.115 ERRORS

(a) If an audit reveals any financial errors in the records provided to the State, the amount in error must be reflected as a credit or debit on the next invoice and subsequent invoices until the amount is paid or refunded in full. However, a credit or debit may not be carried forward for more than four invoices or beyond the termination of the Contract. If a balance remains after four invoices, the remaining amount will be due as a payment or refund within 45 days of the last invoice on which the balance appeared or upon termination of the Contract, whichever is earlier.

(b) In addition to other available remedies, if the difference between the State's actual payment and the correct invoice amount, as determined by an audit, is greater than 10%, the Contractor must pay all reasonable audit costs.

2.120 Warranties

2.121 WARRANTIES AND REPRESENTATIONS

The Contractor represents and warrants:

- (a) It is capable in all respects of fulfilling and must fulfill all of its obligations under this Contract. The performance of all obligations under this Contract must be provided in a timely, professional, and workman-like manner and must meet the performance and operational standards required under this Contract.
- (b) The Contract Appendices, Attachments and Exhibits identify the equipment and software and services necessary for the Deliverable(s) to perform and Services to operate in compliance with the Contract's requirements and other standards of performance.
- (c) It is the lawful owner or licensee of any Deliverable licensed or sold to the State by Contractor or developed by Contractor under this Contract, and Contractor has all of the rights necessary to convey to the State the ownership rights or licensed use, as applicable, of any and all Deliverables. None of the Deliverables provided by Contractor to the State under neither this Contract, nor their use by the State shall infringe the patent, copyright, trade secret, or other proprietary rights of any third party.
- (d) If, under this Contract, Contractor procures any equipment, software or other Deliverable for the State (including equipment, software and other Deliverables manufactured, re-marketed or otherwise sold by Contractor under Contractor's name), then in addition to Contractor's other responsibilities with respect to the items in this Contract, Contractor must assign or otherwise transfer to the State or its designees, or afford the State the benefits of, any manufacturer's warranty for the Deliverable.
- (e) The contract signatory has the power and authority, including any necessary corporate authorizations, necessary to enter into this Contract, on behalf of Contractor.
- (f) It is qualified and registered to transact business in all locations where required.
- (g) Neither the Contractor nor any Affiliates, nor any employee of either, has, must have, or must acquire, any contractual, financial, business, or other interest, direct or indirect, that would conflict in any manner or degree with Contractor's performance of its duties and responsibilities to the State under this Contract or otherwise create an appearance of impropriety with respect to the award or performance of this Agreement. Contractor must notify the State about the nature of the conflict or appearance of impropriety within two days of learning about it.
- (h) Neither Contractor nor any Affiliates, nor any employee of either has accepted or must accept anything of value based on an understanding that the actions of the Contractor or Affiliates or employee on behalf of the State would be influenced. Contractor must not attempt to influence any State employee by the direct or indirect offer of anything of value.
- (i) Neither Contractor nor any Affiliates, nor any employee of either has paid or agreed to pay any person, other than bona fide employees and consultants working solely for Contractor or the Affiliate, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Contract.
- (j) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Bidder; and no attempt was made by Contractor to induce any other person to submit or not submit a proposal for the purpose of restricting competition.
- (k) All financial statements, reports, and other information furnished by Contractor to the State as part of its response to the RFP or otherwise in connection with the award of this Contract fairly and accurately represent the business, properties, financial condition, and results of operations of Contractor as of the respective dates, or for the respective periods, covered by the financial statements, reports, other information. Since the respective dates or periods covered by the

financial statements, reports, or other information, there have been no material adverse changes in the business, properties, financial condition, or results of operations of Contractor.

- (l) All written information furnished to the State by or for the Contractor in connection with this Contract, including its bid, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading.
- (m) It is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State or the department within the previous five years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract.
- (n) If any of the certifications, representations, or disclosures made in the Contractor's original bid response change after contract award, the Contractor is required to report those changes immediately to the Department of Technology, Management & Budget, Procurement.

2.122 WARRANTY OF MERCHANTABILITY

Goods provided by Contractor under this agreement shall be merchantable. All goods provided under this Contract shall be of good quality within the description given by the State, shall be fit for their ordinary purpose, shall be adequately contained and packaged within the description given by the State, shall conform to the agreed upon specifications, and shall conform to the affirmations of fact made by the Contractor or on the container or label.

2.123 WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE

When the Contractor has reason to know or knows any particular purpose for which the goods are required, and the State is relying on the Contractor's skill or judgment to select or furnish suitable goods, there is a warranty that the goods are fit for such purpose.

2.124 WARRANTY OF TITLE

Contractor shall, in providing goods to the State, convey good title in those goods, whose transfer is right and lawful. All goods provided by Contractor shall be delivered free from any security interest, lien, or encumbrance of which the State, at the time of contracting, has no knowledge. Goods provided by Contractor, under this Contract, shall be delivered free of any rightful claim of any third person by of infringement or the like.

2.125 EQUIPMENT WARRANTY

To the extent Contractor is responsible under this Contract for maintaining equipment/system(s), Contractor represents and warrants that it shall maintain the equipment/system(s) in good operating condition and shall undertake all repairs and preventive maintenance according to the applicable manufacturer's recommendations for the period specified in this Contract.

The Contractor represents and warrants that the equipment/system(s) are in good operating condition and operates and performs to the requirements and other standards of performance contained in this Contract, when installed, at the time of Final Acceptance by the State, and for a period of (1) one year commencing upon the first day following Final Acceptance.

Within 60 business days of notification from the State, the Contractor must adjust, repair or replace all equipment that is defective or not performing in compliance with the Contract. The Contractor must assume all costs for replacing parts or units and their installation including transportation and delivery fees, if any.

The Contractor must provide a toll-free telephone number to allow the State to report equipment failures and problems to be remedied by the Contractor.

The Contractor agrees that all warranty service it provides under this Contract must be performed by Original Equipment Manufacturer (OEM) trained, certified and authorized technicians.

The Contractor is the sole point of contact for warranty service. The Contractor warrants that it shall pass through to the State any warranties obtained or available from the original equipment manufacturer, including any replacement, upgraded, or additional equipment warranties.

2.126 EQUIPMENT TO BE NEW

If applicable, all equipment provided under this Contract by Contractor shall be new where Contractor has knowledge regarding whether the equipment is new or assembled from new or serviceable used parts that are like new in performance or has the option of selecting one or the other. Equipment that is assembled from new or serviceable used parts that are like new in performance is acceptable where Contractor does not have knowledge or the ability to select one or other, unless specifically agreed otherwise in writing by the State.

2.127 PROHIBITED PRODUCTS

The State will not accept salvage, distressed, outdated or discontinued merchandise. Shipping of such merchandise to any State agency, as a result of an order placed against the Contract, shall be considered default by the Contractor of the terms and conditions of the Contract and may result in cancellation of the Contract by the State. The brand and product number offered for all items shall remain consistent for the term of the Contract, unless DTMB-Procurement has approved a change order pursuant to **Section 2.024**.

2.128 CONSEQUENCES FOR BREACH

In addition to any remedies available in law, if the Contractor breaches any of the warranties contained in this section, the breach may be considered as a default in the performance of a material obligation of this Contract.

2.130 Insurance

2.13.1 LIABILITY INSURANCE

For the purpose of this Section, "State" includes its departments, divisions, agencies, offices, commissions, officers, employees, and agents.

(a) The Contractor must provide proof that it has obtained the minimum levels of insurance coverage indicated or required by law, whichever is greater. The insurance must protect the State from claims that may arise out of, or result from, or are alleged to arise out of, or result from, the Contractor's or a Subcontractor's performance, including any person directly or indirectly employed by the Contractor or a Subcontractor, or any person for whose acts the Contractor or a Subcontractor may be liable.

(b) The Contractor waives all rights against the State for the recovery of damages that are covered by the insurance policies the Contractor is required to maintain under this Section. The Contractor's failure to obtain and maintain the required insurance will not limit this waiver.

(c) All insurance coverage provided relative to this Contract is primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State.

(d) The State, in its sole discretion, may approve the use of a fully-funded self-insurance program in place of any specified insurance identified in this Section.

(e) Unless the State approves otherwise, any insurer must have an A.M. Best rating of "A" or better and a financial size of VII or better, or if those ratings are not available, a comparable rating from an insurance rating agency approved by the State. All policies of insurance must be issued by companies that have been approved to do business in the State.

(f) Where specific coverage limits are listed in this Section, they represent the minimum acceptable limits. If the Contractor's policy contains higher limits, the State is entitled to coverage to the extent of the higher limits.

(g) The Contractor must maintain all required insurance coverage throughout the term of this Contract and any extensions. However, in the case of claims-made Commercial General Liability policies, the Contractor must secure tail coverage for at least three (3) years following the termination of this Contract.

(h) The Contractor must provide, within five (5) business days, written notice to the Director of DTMB-Procurement if any policy required under this section is cancelled. The notice must include the applicable Contract or Purchase Order number.

(i) The minimum limits of coverage specified are not intended, and may not be construed, to limit any liability or indemnity of the Contractor to any indemnified party or other persons.

(j) The Contractor is responsible for the payment of all deductibles.

(k) If the Contractor fails to pay any premium for a required insurance policy, or if any insurer cancels or significantly reduces any required insurance without the State's approval, the State may, after giving the Contractor at least 30 days' notice, pay the premium or procure similar insurance coverage from another company or companies. The State may deduct any part of the cost from any payment due the Contractor, or require the Contractor to pay that cost upon demand.

(l) In the event the State approves the representation of the State by the insurer's attorney, the attorney may be required to be designated as a Special Assistant Attorney General by the Michigan Attorney General.

(m) The Contractor is required to pay for and provide the type and amount of insurance checked

below:

(i) Commercial General Liability

Minimal Limits:

\$2,000,000 General Aggregate Limit other than Products/Completed Operations

\$2,000,000 Products/Completed Operations Aggregate Limit

\$1,000,000 Personal & Advertising Injury Limit, and

\$1,000,000 Each Occurrence Limit.

Deductible maximum:

\$50,000 Each Occurrence

Additional Requirements:

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the Commercial General Liability certificate. The Contractor also agrees to provide evidence that the insurance policy contains a waiver of subrogation by the insurance company.

The Products/Completed Operations sublimit requirement may be satisfied by evidence of the manufacturer's Commercial General Liability Insurance. The manufacturer must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the Commercial General Liability certificate and must provide evidence that the policy contains a waiver of subrogation by the insurance company.

(ii) Motor Vehicle

Minimal Limits:

If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.

(iii) Workers' Compensation

Minimal Limits:

The Contractor must provide Workers' Compensation coverage according to applicable laws governing work activities in the state of the Contractor's domicile. If the applicable coverage is provided by a self-insurer, the Contractor must provide proof of an approved self-insured authority by the jurisdiction of domicile.

For employees working outside of the state of the Contractor's domicile, the Contractor must provide certificates of insurance proving mandated coverage levels for the jurisdictions where the employees' activities occur.

Additional Requirements:

The Contractor must provide the applicable certificates of insurance and a list of states where the coverage is applicable. Contractor must provide proof that the Workers' Compensation insurance policies contain a waiver of subrogation by the insurance company, except where such a

provision is prohibited or limited by the laws of the jurisdiction in which the work is to be performed.

(iv) Employers Liability

Minimal Limits:

\$100,000 Each Incident
\$100,000 Each Employee by Disease
\$500,000 Aggregate Disease

Additional Requirements:

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the certificate.

(v) Professional Liability (Errors and Omissions)

Minimal Limits:

\$3,000,000 Each Occurrence
\$3,000,000 Annual Aggregate

Deductible Maximum:

\$50,000 Per Loss

(ix) Cyber Liability

Minimal Limits:

\$1,000,000 Each Occurrence
\$1,000,000 Annual Aggregate

Additional Requirements:

Insurance should cover (a) unauthorized acquisition, access, use, physical taking, identity theft, mysterious disappearance, release, distribution or disclosures of personal and corporate information; (b) Transmitting or receiving malicious code via the insured's computer system; (c) Denial of service attacks or the inability to access websites or computer systems.

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the certificate.

2.13.2 SUBCONTRACTOR INSURANCE COVERAGE

Except where the State has approved a subcontract with other insurance provisions, the Contractor must require any Subcontractor to purchase and maintain the insurance coverage required in Section 2.13.1, Liability Insurance. Alternatively, the Contractor may include a Subcontractor under the Contractor's insurance on the coverage required in that Section. The failure of a Subcontractor to comply with insurance requirements does not limit the Contractor's liability or responsibility.

2.13.3 CERTIFICATES OF INSURANCE

Before the Contract is signed, and not less than 20 days before the insurance expiration date every year thereafter, the Contractor must provide evidence that the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents are listed as additional insureds as required. The Contractor must provide DTMB-Procurement with all applicable certificates of insurance verifying insurance coverage or providing, if approved, satisfactory evidence of self-insurance as required in Section 2.13.1, Liability Insurance. Each certificate must be on the standard "Accord" form or equivalent and **MUST IDENTIFY THE APPLICABLE CONTRACT OR PURCHASE ORDER NUMBER.**

2.140 Indemnification

2.141 GENERAL INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from liability, including all claims and losses, and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties), accruing or resulting to any person, firm or corporation that may be injured or damaged by the Contractor in the performance of this Contract and that are attributable to the negligence or tortious acts of the Contractor or any of its subcontractors, or by anyone else for whose acts any of them may be liable.

2.142 CODE INDEMNIFICATION

To the extent permitted by law, the Contractor shall indemnify, defend and hold harmless the State from any claim, loss, or expense arising from Contractor's breach of the No Surreptitious Code Warranty.

2.143 EMPLOYEE INDEMNIFICATION

In any claims against the State of Michigan, its departments, divisions, agencies, sections, commissions, officers, employees and agents, by any employee of the Contractor or any of its subcontractors, the indemnification obligation under the Contract must not be limited in any way by the amount or type of damages, compensation or benefits payable by or for the Contractor or any of its subcontractors under worker's disability compensation acts, disability benefit acts or other employee benefit acts. This indemnification clause is intended to be comprehensive. Any overlap in provisions, or the fact that greater specificity is provided as to some categories of risk, is not intended to limit the scope of indemnification under any other provisions.

2.144 PATENT/COPYRIGHT INFRINGEMENT INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from and against all losses, liabilities, damages (including taxes), and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) incurred in connection with any action or proceeding threatened or brought against the State to the extent that the action or proceeding is based on a claim that any piece of equipment, software, commodity or service supplied by the Contractor or its subcontractors, or the operation of the equipment, software, commodity or service, or the use or reproduction of any documentation provided with the equipment, software, commodity or service infringes any United States patent, copyright, trademark or trade secret of any person or entity, which is enforceable under the laws of the United States.

In addition, should the equipment, software, commodity, or service, or its operation, become or in the State's or Contractor's opinion be likely to become the subject of a claim of infringement, the Contractor must at the Contractor's sole expense (i) procure for the State the right to continue using the equipment, software, commodity or service or, if the option is not reasonably available to the Contractor, (ii) replace or modify to the State's satisfaction the same with equipment, software, commodity or service of equivalent function and performance so that it becomes non-infringing, or, if the option is not reasonably available to Contractor, (iii) accept its return by the State with appropriate credits to the State against the Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

Notwithstanding the foregoing, the Contractor has no obligation to indemnify or defend the State for, or to pay any costs, damages or attorneys' fees related to, any claim based upon (i) equipment developed based on written specifications of the State; (ii) use of the equipment in a configuration other than implemented or approved in writing by the Contractor, including, but not limited to, any modification of the equipment by the State; or (iii) the combination, operation, or use of the equipment with equipment or software not supplied by the Contractor under this Contract.

2.145 CONTINUATION OF INDEMNIFICATION OBLIGATIONS

The Contractor's duty to indemnify under this Section continues in full force and effect, notwithstanding the expiration or early cancellation of the Contract, with respect to any claims based on facts or conditions that occurred before expiration or cancellation.

2.146 INDEMNIFICATION PROCEDURES

The procedures set forth below must apply to all indemnity obligations under this Contract.

- (a) After the State receives notice of the action or proceeding involving a claim for which it shall seek indemnification, the State must promptly notify Contractor of the claim in writing and take or assist Contractor in taking, as the case may be, any reasonable action to avoid the imposition of a default judgment against Contractor. No failure to notify the Contractor relieves the Contractor of its indemnification obligations except to the extent that the Contractor can prove damages attributable to the failure. Within 10 days following receipt of written notice from the State relating to any claim, the Contractor must notify the State in writing whether Contractor agrees to assume control of the defense and settlement of that claim (a "Notice of Election"). After notifying Contractor of a claim and before the State receiving Contractor's Notice of Election, the State is entitled to defend against the claim, at the Contractor's expense, and the Contractor will be responsible for any reasonable costs incurred by the State in defending against the claim during that period.
- (b) If Contractor delivers a Notice of Election relating to any claim: (i) the State is entitled to participate in the defense of the claim and to employ counsel at its own expense to assist in the handling of the claim and to monitor and advise the State about the status and progress of the defense; (ii) the Contractor must, at the request of the State, demonstrate to the reasonable satisfaction of the State, the Contractor's financial ability to carry out its defense and indemnity obligations under this Contract; (iii) the Contractor must periodically advise the State about the status and progress of the defense and must obtain the prior written approval of the State before entering into any settlement of the claim or ceasing to defend against the claim; and (iv) to the extent that any principles of Michigan governmental or public law may be involved or challenged, the State has the right, at its own expense, to control the defense of that portion of the claim involving the principles of Michigan governmental or public law. But the State may retain control of the defense and settlement of a claim by notifying the Contractor in writing within 10 days after the State's receipt of Contractor's information requested by the State under clause (ii) of this paragraph if the State determines that the Contractor has failed to demonstrate to the reasonable satisfaction of the State the Contractor's financial ability to carry out its defense and indemnity obligations under this Section. Any litigation activity on behalf of the State, or any of its subdivisions under this Section, must be coordinated with the Department of Attorney General. In the event the insurer's attorney represents the State under this Section, the insurer's attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.
- (c) If Contractor does not deliver a Notice of Election relating to any claim of which it is notified by the State as provided above, the State may defend the claim in the manner as it may deem appropriate, at the cost and expense of Contractor. If it is determined that the claim was one against which Contractor was required to indemnify the State, upon request of the State, Contractor must promptly reimburse the State for all the reasonable costs and expenses.

2.150 Termination/Cancellation

2.151 NOTICE AND RIGHT TO CURE

If the Contractor breaches the contract, and the State in its sole discretion determines that the breach is curable, then the State shall provide the Contractor with written notice of the breach and a time period (not less than 30 days) to cure the Breach. The notice of breach and opportunity to cure is inapplicable for successive or repeated breaches or if the State determines in its sole discretion that the breach poses a serious and imminent threat to the health or safety of any person or the imminent loss, damage, or destruction of any real or tangible personal property.

2.152 TERMINATION FOR CAUSE

- (a) The State may terminate this contract, for cause, by notifying the Contractor in writing, if the Contractor (i) breaches any of its material duties or obligations under this Contract (including a

Chronic Failure to meet any particular SLA), or (ii) fails to cure a breach within the time period specified in the written notice of breach provided by the State

- (b) If this Contract is terminated for cause, the Contractor must pay all costs incurred by the State in terminating this Contract, including but not limited to, State administrative costs, reasonable attorneys' fees and court costs, and any reasonable additional costs the State may incur to procure the Services/Deliverables required by this Contract from other sources. Re-procurement costs are not consequential, indirect or incidental damages, and cannot be excluded by any other terms otherwise included in this Contract, provided the costs are not in excess of 50% more than the prices for the Service/Deliverables provided under this Contract.
- (c) If the State chooses to partially terminate this Contract for cause, charges payable under this Contract shall be equitably adjusted to reflect those Services/Deliverables that are terminated and the State must pay for all Services/Deliverables for which Final Acceptance has been granted provided up to the termination date. Services and related provisions of this Contract that are terminated for cause must cease on the effective date of the termination.
- (d) If the State terminates this Contract for cause under this Section, and it is determined, for any reason, that Contractor was not in breach of contract under the provisions of this section, that termination for cause must be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties must be limited to that otherwise provided in this Contract for a termination for convenience.

2.153 TERMINATION FOR CONVENIENCE

The State may terminate this Contract for its convenience, in whole or part, if the State determines that a termination is in the State's best interest. Reasons for the termination must be left to the sole discretion of the State and may include, but not necessarily be limited to (a) the State no longer needs the Services or products specified in the Contract, (b) relocation of office, program changes, changes in laws, rules, or regulations make implementation of the Services no longer practical or feasible, (c) unacceptable prices for Additional Services or New Work requested by the State, or (d) falsification or misrepresentation, by inclusion or non-inclusion, of information material to a response to any RFP issued by the State. The State may terminate this Contract for its convenience, in whole or in part, by giving Contractor written notice at least 30 days before the date of termination. If the State chooses to terminate this Contract in part, the charges payable under this Contract must be equitably adjusted to reflect those Services/Deliverables that are terminated. Services and related provisions of this Contract that are terminated for convenience must cease on the effective date of the termination.

2.154 TERMINATION FOR NON-APPROPRIATION

- (a) Contractor acknowledges that, if this Contract extends for several fiscal years, continuation of this Contract is subject to appropriation or availability of funds for this Contract. If funds to enable the State to effect continued payment under this Contract are not appropriated or otherwise made available, the State must terminate this Contract and all affected Statements of Work, in whole or in part, at the end of the last period for which funds have been appropriated or otherwise made available by giving written notice of termination to Contractor. The State must give Contractor at least 30 days advance written notice of termination for non-appropriation or unavailability (or the time as is available if the State receives notice of the final decision less than 30 days before the funding cutoff).
- (b) If funding for the Contract is reduced by law, or funds to pay Contractor for the agreed-to level of the Services or production of Deliverables to be provided by Contractor are not appropriated or otherwise unavailable, the State may, upon 30 days written notice to Contractor, reduce the level of the Services or change the production of Deliverables in the manner and for the periods of time as the State may elect. The charges payable under this Contract shall be equitably adjusted to reflect any equipment, services or commodities not provided by reason of the reduction.
- (c) If the State terminates this Contract, eliminates certain Deliverables, or reduces the level of Services to be provided by Contractor under this Section, the State must pay Contractor for all Work-in-Process performed through the effective date of the termination or reduction in level, as the case may be and as determined by the State, to the extent funds are available. This Section shall not preclude Contractor from reducing or stopping Services/Deliverables or raising against the State in a court of competent jurisdiction, any claim for a shortfall in payment for Services performed or Deliverables finally accepted before the effective date of termination.

2.155 TERMINATION FOR CRIMINAL CONVICTION

The State may terminate this Contract immediately and without further liability or penalty in the event Contractor, an officer of Contractor, or an owner of a 25% or greater share of Contractor is convicted of a criminal offense related to a State, public or private Contract or subcontract.

2.156 TERMINATION FOR APPROVALS RESCINDED

The State may terminate this Contract if any final administrative or judicial decision or adjudication disapproves a previously approved request for purchase of personal services under Constitution 1963, Article 11, § 5, and Civil Service Rule 7-1. In that case, the State shall pay the Contractor for only the work completed to that point under the Contract. Termination may be in whole or in part and may be immediate as of the date of the written notice to Contractor or may be effective as of the date stated in the written notice.

2.157 RIGHTS AND OBLIGATIONS UPON TERMINATION

- (a) If the State terminates this Contract for any reason, the Contractor must (a) stop all work as specified in the notice of termination, (b) take any action that may be necessary, or that the State may direct, for preservation and protection of Deliverables or other property derived or resulting from this Contract that may be in Contractor's possession, (c) return all materials and property provided directly or indirectly to Contractor by any entity, agent or employee of the State, (d) transfer title in, and deliver to, the State, unless otherwise directed, all Deliverables intended to be transferred to the State at the termination of the Contract and which are resulting from the Contract (which must be provided to the State on an "As-Is" basis except to the extent the amounts paid by the State in respect of the items included compensation to Contractor for the provision of warranty services in respect of the materials), and (e) take any action to mitigate and limit any potential damages, or requests for Contractor adjustment or termination settlement costs, to the maximum practical extent, including terminating or limiting as otherwise applicable those subcontracts and outstanding orders for material and supplies resulting from the terminated Contract.
- (b) If the State terminates this Contract before its expiration for its own convenience, the State must pay Contractor for all charges due for Services provided before the date of termination and, if applicable, as a separate item of payment under this Contract, for Work In Process, on a percentage of completion basis at the level of completion determined by the State. All completed or partially completed Deliverables prepared by Contractor under this Contract, at the option of the State, becomes the State's property, and Contractor is entitled to receive equitable fair compensation for the Deliverables. Regardless of the basis for the termination, the State is not obligated to pay, or otherwise compensate, Contractor for any lost expected future profits, costs or expenses incurred with respect to Services not actually performed for the State.
- (c) Upon a good faith termination, the State may assume, at its option, any subcontracts and agreements for services and deliverables provided under this Contract, and may further pursue completion of the Services/Deliverables under this Contract by replacement contract or otherwise as the State may in its sole judgment deem expedient.

2.158 RESERVATION OF RIGHTS

Any termination of this Contract or any Statement of Work issued under it by a party must be with full reservation of, and without prejudice to, any rights or remedies otherwise available to the party with respect to any claims arising before or as a result of the termination.

2.160 Termination by Contractor

2.161 TERMINATION BY CONTRACTOR

If the State breaches the Contract, and the Contractor in its sole discretion determines that the breach is curable, then the Contractor will provide the State with written notice of the breach and a time period (not less than 30 days) to cure the breach. The Notice of Breach and opportunity to cure is inapplicable for successive and repeated breaches.

The Contractor may terminate this Contract if the State (i) materially breaches its obligation to pay the Contractor undisputed amounts due and owing under this Contract, (ii) breaches its other obligations under this Contract to an extent that makes it impossible or commercially impractical for the Contractor to perform the Services, or (iii) does not cure the breach within the time period specified in a written notice of breach. But the Contractor must discharge its obligations under **Section 2.160** before it terminates the Contract.

2.170 Transition Responsibilities

2.171 CONTRACTOR TRANSITION RESPONSIBILITIES

If the State terminates this contract, for convenience or cause, or if the Contract is otherwise dissolved, voided, rescinded, nullified, expires or rendered unenforceable, the Contractor shall comply with direction provided by the State to assist in the orderly transition of equipment, services, software, leases, etc. to the State or a third party designated by the State. If this Contract expires or terminates, the Contractor agrees to make all reasonable efforts to effect an orderly transition of services within a reasonable period of time that in no event will exceed 30 days. These efforts must include, but are not limited to, those listed in **Section 2.150**.

2.172 CONTRACTOR PERSONNEL TRANSITION

The Contractor shall work with the State, or a specified third party, to develop a transition plan setting forth the specific tasks and schedule to be accomplished by the parties, to effect an orderly transition. The Contractor must allow as many personnel as practicable to remain on the job to help the State, or a specified third party, maintain the continuity and consistency of the services required by this Contract. In addition, during or following the transition period, in the event the State requires the Services of the Contractor's subcontractors or vendors, as necessary to meet its needs, Contractor agrees to reasonably, and with good-faith, work with the State to use the Services of Contractor's subcontractors or vendors. Contractor will notify all of Contractor's subcontractors of procedures to be followed during transition.

2.173 CONTRACTOR INFORMATION TRANSITION

The Contractor shall provide reasonable detailed specifications for all Services/Deliverables needed by the State, or specified third party, to properly provide the Services/Deliverables required under this Contract. The Contractor will provide the State with asset management data generated from the inception of this Contract through the date on which this Contractor is terminated in a comma-delineated format unless otherwise requested by the State. The Contractor will deliver to the State any remaining owed reports and documentation still in Contractor's possession subject to appropriate payment by the State.

2.174 CONTRACTOR SOFTWARE TRANSITION

The Contractor shall reasonably assist the State in the acquisition of any Contractor software required to perform the Services/use the Deliverables under this Contract. This must include any documentation being used by the Contractor to perform the Services under this Contract. If the State transfers any software licenses to the Contractor, those licenses must, upon expiration of the Contract, transfer back to the State at their current revision level. Upon notification by the State, Contractor may be required to freeze all non-critical changes to Deliverables/Services.

2.175 TRANSITION PAYMENTS

If the transition results from a termination for any reason, the termination provisions of this Contract must govern reimbursement. If the transition results from expiration, the Contractor will be reimbursed for all reasonable transition costs (i.e. costs incurred within the agreed period after contract expiration that result from transition operations) at the rates agreed upon by the State. The Contractor will prepare an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

2.176 STATE TRANSITION RESPONSIBILITIES

In the event that this Contract is terminated, dissolved, voided, rescinded, nullified, or otherwise rendered unenforceable, the State agrees to reconcile all accounts between the State and the Contractor, complete

any pending post-project reviews and perform any others obligations upon which the State and the Contractor agree.

- (a) Reconciling all accounts between the State and the Contractor;
- (b) Completing any pending post-project reviews.

2.180 Stop Work

2.181 STOP WORK ORDERS

The State may, at any time, by written Stop Work Order to Contractor, require that Contractor stop all, or any part, of the work called for by the Contract for a period of up to 90 calendar days after the Stop Work Order is delivered to Contractor, and for any further period to which the parties may agree. The Stop Work Order must be identified as a Stop Work Order and must indicate that it is issued under this **Section**. Upon receipt of the stop work order, Contractor must immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work stoppage. Within the period of the stop work order, the State must either: (a) cancel the stop work order; or (b) terminate the work covered by the Stop Work Order as provided in **Section 2.182**.

2.182 CANCELLATION OR EXPIRATION OF STOP WORK ORDER

The Contractor shall resume work if the State cancels a Stop Work Order or if it expires. The parties shall agree upon an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract shall be modified, in writing, accordingly, if: (a) the Stop Work Order results in an increase in the time required for, or in Contractor's costs properly allocable to, the performance of any part of the Contract; and (b) Contractor asserts its right to an equitable adjustment within 30 calendar days after the end of the period of work stoppage; provided that, if the State decides the facts justify the action, the State may receive and act upon a Contractor proposal submitted at any time before final payment under the Contract. Any adjustment will conform to the requirements of **Section 2.024**.

2.183 ALLOWANCE OF CONTRACTOR COSTS

If the Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated for reasons other than material breach, the termination shall be deemed to be a termination for convenience under **Section 2.153**, and the State shall pay reasonable costs resulting from the Stop Work Order in arriving at the termination settlement. For the avoidance of doubt, the State shall not be liable to Contractor for loss of profits because of a Stop Work Order issued under this Section.

2.190 Dispute Resolution

2.191 IN GENERAL

Any claim, counterclaim, or dispute between the State and Contractor arising out of or relating to the Contract or any Statement of Work must be resolved as follows. For all Contractor claims seeking an increase in the amounts payable to Contractor under the Contract, or the time for Contractor's performance, Contractor must submit a letter, together with all data supporting the claims, executed by Contractor's Contract Administrator or the Contract Administrator's designee certifying that (a) the claim is made in good faith, (b) the amount claimed accurately reflects the adjustments in the amounts payable to Contractor or the time for Contractor's performance for which Contractor believes the State is liable and covers all costs of every type to which Contractor is entitled from the occurrence of the claimed event, and (c) the claim and the supporting data are current and complete to Contractor's best knowledge and belief.

2.192 INFORMAL DISPUTE RESOLUTION

(a) All disputes between the parties shall be resolved under the Contract Management procedures in this Contract. If the parties are unable to resolve any dispute after compliance with the processes, the

parties must meet with the Director of Procurement, DTMB, or designee, to resolve the dispute without the need for formal legal proceedings, as follows:

- (1) The representatives of Contractor and the State must meet as often as the parties reasonably deem necessary to gather and furnish to each other all information with respect to the matter at issue which the parties believe to be appropriate and germane in connection with its resolution. The representatives shall discuss the problem and negotiate in good faith in an effort to resolve the dispute without the necessity of any formal proceeding.
 - (2) During the course of negotiations, all reasonable requests made by one party to another for non-privileged information reasonably related to the Contract shall be honored in order that each of the parties may be fully advised of the other's position.
 - (3) The specific format for the discussions shall be left to the discretion of the designated State and Contractor representatives, but may include the preparation of agreed upon statements of fact or written statements of position.
 - (4) Following the completion of this process within 60 calendar days, the Director of Procurement, DTMB, or designee, shall issue a written opinion regarding the issue(s) in dispute within 30 calendar days. The opinion regarding the dispute must be considered the State's final action and the exhaustion of administrative remedies.
- (b) This Section shall not be construed to prevent either party from instituting, and a party is authorized to institute, formal proceedings earlier to avoid the expiration of any applicable limitations period, to preserve a superior position with respect to other creditors, or under Section 2.193.
- (c) The State shall not mediate disputes between the Contractor and any other entity, except state agencies, concerning responsibility for performance of work under the Contract.

2.193 INJUNCTIVE RELIEF

A claim between the State and the Contractor is not subject to the provisions of Section 2.192, Informal Dispute Resolution, where a party makes a good faith determination that a breach of the Contract by the other party will result in damages so immediate, so large or severe, and so incapable of adequate redress that a temporary restraining order or other injunctive relief is the only adequate remedy.

2.194 CONTINUED PERFORMANCE

Each party agrees to continue performing its obligations under the Contract while a dispute is being resolved except to the extent the issue in dispute precludes performance (dispute over payment must not be deemed to preclude performance) and without limiting either party's right to terminate the Contract as provided in **Section 2.150**, as the case may be.

2.200 Federal and State Contract Requirements

2.201 NONDISCRIMINATION

In the performance of the Contract, Contractor agrees not to discriminate against any employee or applicant for employment, with respect to his or her hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of race, color, religion, national origin, ancestry, age, sex, height, weight, and marital status, physical or mental disability. Contractor further agrees that every subcontract entered into for the performance of this Contract or any purchase order resulting from this Contract will contain a provision requiring non-discrimination in employment, as specified here, binding upon each Subcontractor. This covenant is required under the Elliot Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, et seq., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., and any breach of this provision may be regarded as a material breach of the Contract.

2.202 UNFAIR LABOR PRACTICES

Under 1980 PA 278, MCL 423.321, et seq., the State shall not award a Contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled under section 2 of the Act. This information is compiled by the United States National Labor Relations Board. A Contractor of the State, in relation to the Contract, shall not enter into a

contract with a Subcontractor, manufacturer, or supplier whose name appears in this register. Under section 4 of 1980 PA 278, MCL 423.324, the State may void any Contract if, after award of the Contract, the name of Contractor as an employer or the name of the Subcontractor, manufacturer or supplier of Contractor appears in the register.

2.203 WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT

In performing Services for the State, the Contractor shall comply with the Department of Civil Services Rule 2-20 regarding Workplace Safety and Rule 1-8.3 regarding Discriminatory Harassment. In addition, the Contractor shall comply with Civil Service regulations and any applicable agency rules provided to the Contractor. For Civil Service Rules, see <http://www.mi.gov/mdcs/0,1607,7-147-6877---,00.html>.

2.204 PREVAILING WAGE

Wages rates and fringe benefits to be paid each class of individuals employed by the Contractor, its subcontractors, their subcontractors, and all persons involved with the performance of this Contract in privity of contract with the Contractor shall not be less than the wage rates and fringe benefits established by the Michigan Department of Licensing and Regulatory Affairs, Wage and Hour Division, schedule of occupational classification and wage rates and fringe benefits for the local where the work is to be performed. The term Contractor shall include all general contractors, prime contractors, project managers, trade contractors, and all of their contractors or subcontractors and persons in privity of contract with them.

The Contractor, its subcontractors, their subcontractors and all persons involved with the performance of this contract in privity of contract with the Contractor shall keep posted on the work site, in a conspicuous place, a copy of all wage rates and fringe benefits as prescribed in the Contract. Contractor shall also post, in a conspicuous place, the address and telephone number of the Michigan Department of Licensing and Regulatory Affairs, the agency responsible for enforcement of the wage rates and fringe benefits. Contractor shall keep an accurate record showing the name and occupation of the actual wage and benefits paid to each individual employed in connection with this contract. This record shall be available to the State upon request for reasonable inspection.

If any trade is omitted from the list of wage rates and fringe benefits to be paid to each class of individuals by the Contractor, it is understood that the trades omitted shall also be paid not less than the wage rate and fringe benefits prevailing in the local where the work is to be performed.

2.210 Governing Law

2.211 GOVERNING LAW

The Contract shall in all respects be governed by, and construed according to, the substantive laws of the State of Michigan without regard to any Michigan choice of law rules that would apply the substantive law of any other jurisdiction to the extent not inconsistent with, or pre-empted by federal law.

2.212 COMPLIANCE WITH LAWS

Contractor shall comply with all applicable state, federal and local laws and ordinances in providing the Services/Deliverables.

2.213 JURISDICTION

Any dispute arising from the Contract shall be resolved in the State of Michigan. With respect to any claim between the parties, Contractor consents to venue in Ingham County, Michigan, and irrevocably waives any objections it may have to the jurisdiction on the grounds of lack of personal jurisdiction of the court or the laying of venue of the court or on the basis of forum non conveniens or otherwise. Contractor agrees to appoint agents in the State of Michigan to receive service of process.

2.220 Limitation of Liability

2.221 LIMITATION OF LIABILITY

Neither the Contractor nor the State is liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages. This limitation of liability does not apply to claims for infringement of United States patent, copyright, trademark or trade secrets; to claims for personal injury or damage to property caused by the gross negligence or willful misconduct of the Contractor; to claims covered by other specific provisions of this Contract calling for liquidated damages; or to court costs or attorneys' fees awarded by a court in addition to damages after litigation based on this Contract.

2.230 Disclosure Responsibilities

2.231 DISCLOSURE OF LITIGATION

Contractor shall disclose any material criminal litigation, investigations or proceedings involving the Contractor (and each Subcontractor) or any of its officers or directors or any litigation, investigations or proceedings under the Sarbanes-Oxley Act. In addition, each Contractor (and each Subcontractor) shall notify the State of any material civil litigation, arbitration or proceeding which arises during the term of the Contract and extensions, to which Contractor (or, to the extent Contractor is aware, any Subcontractor) is a party, and which involves: (i) disputes that might reasonably be expected to adversely affect the viability or financial stability of Contractor or any Subcontractor; or (ii) a claim or written allegation of fraud against Contractor or, to the extent Contractor is aware, any Subcontractor by a governmental or public entity arising out of their business dealings with governmental or public entities. The Contractor shall disclose in writing to the Contract Administrator any litigation, investigation, arbitration or other proceeding (collectively, "Proceeding") within 30 days of its occurrence. Details of settlements that are prevented from disclosure by the terms of the settlement may be annotated. Information provided to the State from Contractor's publicly filed documents referencing its material litigation shall be deemed to satisfy the requirements of this Section.

If any Proceeding disclosed to the State under this Section, or of which the State otherwise becomes aware, during the term of this Contract would cause a reasonable party to be concerned about:

- (a) the ability of Contractor (or a Subcontractor) to continue to perform this Contract according to its terms and conditions, or
- (b) whether Contractor (or a Subcontractor) in performing Services for the State is engaged in conduct which is similar in nature to conduct alleged in the Proceeding, which conduct would constitute a breach of this Contract or a violation of Michigan law, regulations or public policy, then the Contractor must provide the State all reasonable assurances requested by the State to demonstrate that:
 - (1) Contractor and its Subcontractors will be able to continue to perform this Contract and any Statements of Work according to its terms and conditions, and
 - (2) Contractor and its Subcontractors have not and will not engage in conduct in performing the Services which is similar in nature to the conduct alleged in the Proceeding.
- (c) Contractor shall make the following notifications in writing:
 - (1) Within 30 days of Contractor becoming aware that a change in its ownership or officers has occurred, or is certain to occur, or a change that could result in changes in the valuation of its capitalized assets in the accounting records, Contractor must notify DTMB-Procurement.
 - (2) Contractor shall also notify DTMB Procurement within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership or officers.
 - (3) Contractor shall also notify DTMB-Procurement within 30 days whenever changes to company affiliations occur.

2.232 CALL CENTER DISCLOSURE

Contractor and/or all subcontractors involved in the performance of this Contract providing call or contact center services to the State shall disclose the location of its call or contact center services to inbound callers. Failure to disclose this information is a material breach of this Contract.

2.233 BANKRUPTCY

The State may, without prejudice to any other right or remedy, terminate this Contract, in whole or in part, and, at its option, may take possession of the "Work in Process" and finish the Works in Process by whatever appropriate method the State may deem expedient if:

- (a) the Contractor files for protection under the bankruptcy laws;
- (b) an involuntary petition is filed against the Contractor and not removed within 30 days;
- (c) the Contractor becomes insolvent or if a receiver is appointed due to the Contractor's insolvency;
- (d) the Contractor makes a general assignment for the benefit of creditors; or
- (e) the Contractor or its affiliates are unable to provide reasonable assurances that the Contractor or its affiliates can deliver the services under this Contract.

Contractor will fix appropriate notices or labels on the Work in Process to indicate ownership by the State. To the extent reasonably possible, materials and Work in Process shall be stored separately from other stock and marked conspicuously with labels indicating ownership by the State.

2.240 Performance

2.241 TIME OF PERFORMANCE

- (a) Contractor shall use commercially reasonable efforts to provide the resources necessary to complete all Services and Deliverables according to the time schedules contained in the Statements of Work and other Exhibits governing the work, and with professional quality.
- (b) Without limiting the generality of **Section 2.241**, Contractor shall notify the State in a timely manner upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion of any Deliverables/Services on the scheduled due dates in the latest State-approved delivery schedule and must inform the State of the projected actual delivery date.
- (c) If the Contractor believes that a delay in performance by the State has caused or will cause the Contractor to be unable to perform its obligations according to specified Contract time periods, the Contractor must notify the State in a timely manner and must use commercially reasonable efforts to perform its obligations according to the Contract time periods notwithstanding the State's failure. Contractor will not be in default for a delay in performance to the extent the delay is caused by the State.

2.242 SERVICE LEVEL AGREEMENT (SLA)

- (a) SLAs will be completed with the following operational considerations:
 - (1) SLAs will not be calculated for individual Incidents where any event of Excusable Failure has been determined; Incident means any interruption in Services.
 - (2) SLAs will not be calculated for individual Incidents where loss of service is planned and where the State has received prior notification or coordination.
 - (3) SLAs will not apply if the applicable Incident could have been prevented through planning proposed by Contractor and not implemented at the request of the State. To invoke this consideration, complete documentation relevant to the denied planning proposal must be presented to substantiate the proposal.
 - (4) Time period measurements will be based on the time Incidents are received by the Contractor and the time that the State receives notification of resolution based on 24x7x365 time period, except that the time period measurement will be suspended based on the following:
 - (i) Time period(s) will not apply where Contractor does not have access to a physical State Location and where access to the State Location is necessary for problem identification and resolution.

- (ii) Time period(s) will not apply where Contractor needs to obtain timely and accurate information or appropriate feedback and is unable to obtain timely and accurate information or appropriate feedback from the State.
- (b) Chronic Failure for any Service(s) will be defined as three unscheduled outage(s) or interruption(s) on any individual Service for the same reason or cause or if the same reason or cause was reasonably discoverable in the first instance over a rolling 30 day period. Chronic Failure will result in the State's option to terminate the effected individual Service(s) and procure them from a different vendor for the chronic location(s) with Contractor to pay the difference in charges for up to three additional months. The termination of the Service will not affect any tiered pricing levels.
- (c) Root Cause Analysis will be performed on any Business Critical outage(s) or outage(s) on Services when requested by the Contract Administrator. Contractor will provide its analysis within two weeks of outage(s) and provide a recommendation for resolution.
- (d) All decimals must be rounded to two decimal places with five and greater rounding up and four and less rounding down unless otherwise specified.

2.243 LIQUIDATED DAMAGES

The parties acknowledge that late or improper completion of the Work will cause loss and damage to the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result. Therefore, Contractor and the State agree that if there is late or improper completion of the Work and the State does not elect to exercise its rights under **Section 2.152**, the State is entitled to collect liquidated damages in the amount of \$5,000.00 and an additional \$100.00 per day for each day Contractor fails to remedy the late or improper completion of the Work.

Unauthorized Removal of any Key Personnel

It is acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of the Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 2.152**, the State may assess liquidated damages against Contractor as specified below.

For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the liquidated damages amount is \$25,000.00 per individual if the Contractor identifies a replacement approved by the State under **Section 2.060** and assigns the replacement to the Project to shadow the Key Personnel who is leaving for a period of at least 30 days before the Key Personnel's removal.

If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 days, in addition to the \$25,000.00 liquidated damages for an Unauthorized Removal, Contractor must pay the amount of \$833.33 per day for each day of the 30 day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to \$25,000.00 maximum per individual. The total liquidated damages that may be assessed per Unauthorized Removal and failure to provide 30 days of shadowing must not exceed \$50,000.00 per individual.

2.244 EXCUSABLE FAILURE

Neither party will be liable for any default, damage or delay in the performance of its obligations under the Contract to the extent the default, damage or delay is caused by government regulations or requirements (executive, legislative, judicial, military or otherwise), power failure, electrical surges or current fluctuations, lightning, earthquake, war, water or other forces of nature or acts of God, delays or failures of transportation, equipment shortages, suppliers' failures, or acts or omissions of common carriers, fire; riots, civil disorders; strikes or other labor disputes, embargoes; injunctions (provided the injunction was not issued as a result of any fault or negligence of the party seeking to have its default or delay excused); or any other cause beyond the reasonable control of a party; provided the non-performing party and its Subcontractors are without fault in causing the default or delay, and the default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of alternate sources, workaround plans or other means, including disaster recovery plans.

If a party does not perform its contractual obligations for any of the reasons listed above, the non-performing party will be excused from any further performance of its affected obligation(s) for as long as the circumstances prevail. But the party must use commercially reasonable efforts to recommence performance whenever and to whatever extent possible without delay. A party must promptly notify the other party in writing immediately after the excusable failure occurs, and also when it abates or ends.

If any of the above-enumerated circumstances substantially prevent, hinder, or delay the Contractor's performance of the Services/provision of Deliverables for more than 10 Business Days, and the State determines that performance is not likely to be resumed within a period of time that is satisfactory to the State in its reasonable discretion, then at the State's option: (a) the State may procure the affected Services/Deliverables from an alternate source, and the State is not be liable for payment for the unperformed Services/ Deliverables not provided under the Contract for so long as the delay in performance continues; (b) the State may terminate any portion of the Contract so affected and the charges payable will be equitably adjusted to reflect those Services/Deliverables terminated; or (c) the State may terminate the affected Statement of Work without liability to Contractor as of a date specified by the State in a written notice of termination to the Contractor, except to the extent that the State must pay for Services/Deliverables provided through the date of termination.

The Contractor will not have the right to any additional payments from the State as a result of any Excusable Failure occurrence or to payments for Services not rendered/Deliverables not provided as a result of the Excusable Failure condition. Defaults or delays in performance by Contractor which are caused by acts or omissions of its Subcontractors will not relieve Contractor of its obligations under the Contract except to the extent that a Subcontractor is itself subject to an Excusable Failure condition described above and Contractor cannot reasonably circumvent the effect of the Subcontractor's default or delay in performance through the use of alternate sources, workaround plans or other means.

2.250 Approval of Deliverables

2.251 DELIVERY OF DELIVERABLES

A list of the Deliverables to be prepared and delivered by Contractor including, for each Deliverable, the scheduled delivery date and a designation of whether the Deliverable is a document ("Written Deliverable") or a Custom Software Deliverable is attached, if applicable. All Deliverables shall be completed and delivered for State review and written approval and, where applicable, installed in accordance with the State-approved delivery schedule and any other applicable terms and conditions of this Contract.

Prior to delivering any Deliverable to the State, Contractor will first perform all required quality assurance activities, and, in the case of Custom Software Deliverables, System Testing to verify that the Deliverable is complete and in conformance with its specifications. Before delivering a Deliverable to the State, Contractor shall certify to the State that (1) it has performed such quality assurance activities, (2) it has performed any applicable testing, (3) it has corrected all material deficiencies discovered during such quality assurance activities and testing, (4) the Deliverable is in a suitable state of readiness for the State's review and approval, and (5) the Deliverable/Service has all Critical Security patches/updates applied.

In discharging its obligations under this Section, Contractor shall be at all times (except where the parties agree otherwise in writing) in compliance with Level 3 of the Software Engineering Institute's Capability Maturity Model for Software ("CMM Level 3") or its equivalent.

2.252 CONTRACTOR SYSTEM TESTING

Contractor will be responsible for System Testing each Custom Software Deliverable in Contractor's development environment prior to turning over the Custom Software Deliverable to the State for User Acceptance Testing and approval. Contractor's System Testing shall include the following, at a minimum, plus any other testing required by CMM Level 3 or Contractor's system development methodology:

Contractor will be responsible for performing Unit Testing and incremental Integration Testing of the components of each Custom Software Deliverable.

Contractor's System Testing will also include Integration Testing of each Custom Software Deliverable to ensure proper inter-operation with all prior software Deliverables, interfaces and other components that are intended to inter-operate with such Custom Software Deliverable, and will include Regression Testing, volume and stress testing to ensure that the Custom Software Deliverables are able to meet the State's projected growth in the number and size of transactions to be processed by the Application and number of users, as such projections are set forth in the applicable Statement of Work.

Contractor's System Testing will also include Business Function Testing and Technical Testing of each Application in a simulated production environment. Business Function Testing will include testing of full work streams that flow through the Application as the Application will be incorporated within the State's computing environment. The State shall participate in and provide support for the Business Function Testing to the extent reasonably requested by Contractor. Within ten (10) days before the commencement of Business Function Testing pursuant to this Section, Contractor shall provide the State for State review and written approval Contractor's test plan for Business Function Testing.

Within five (5) Business Days following the completion of System Testing pursuant to this **Section**, Contractor shall provide to the State a testing matrix establishing that testing for each condition identified in the System Testing plans has been conducted and successfully concluded. To the extent that testing occurs on State premises, the State shall be entitled to observe or otherwise participate in testing under this Section as the State may elect.

2.253 APPROVAL OF DELIVERABLES, IN GENERAL

All Deliverables (Written Deliverables and Custom Software Deliverables) require formal written approval by the State, in accordance with the following procedures. Formal approval by the State requires that the Deliverable be confirmed in writing by the State to meet its specifications, which, in the case of Custom Software Deliverables, will include the successful completion of State User Acceptance Testing, to be led by the State with the support and assistance of Contractor. The parties acknowledge that the approval process set forth herein will be facilitated by ongoing consultation between the parties, visibility of interim and intermediate Deliverables and collaboration on key decisions.

The State's obligation to comply with any State Review Period is conditioned on the timely delivery of Deliverables being reviewed. If Contractor fails to provide a Deliverable to the State in a timely manner, the State will nevertheless use commercially reasonable efforts to complete its review or testing within the applicable State Review Period.

Before commencement of its review or testing of a Deliverable, the State may inspect the Deliverable to confirm that all components of the Deliverable (e.g., software, associated documentation, and other materials) have been delivered. If the State determines that the Deliverable is incomplete, the State may refuse delivery of the Deliverable without performing any further inspection or testing of the Deliverable. Otherwise, the review period will be deemed to have started on the day the State receives the Deliverable and the applicable certification by Contractor in accordance with this Section.

The State will approve in writing a Deliverable upon confirming that it conforms to and, in the case of a Custom Software Deliverable, performs in accordance with, its specifications without material deficiency. The State may, but shall not be required to, conditionally approve in writing a Deliverable that contains material deficiencies if the State elects to permit Contractor to rectify them post-approval. In any case, Contractor will be responsible for working diligently to correct within a reasonable time at Contractor's expense all deficiencies in the Deliverable that remain outstanding at the time of State approval.

If, after three (3) opportunities (the original and two repeat efforts), Contractor is unable to correct all deficiencies preventing State approval of a Deliverable, the State may: (i) demand that Contractor cure the failure and give Contractor additional time to cure the failure at the sole expense of Contractor; or (ii) keep this Contract in force and do, either itself or through other parties, whatever Contractor has failed to do, in which event Contractor shall bear any excess expenditure incurred by the State in so doing beyond the contract price for such Deliverable and will pay the State an additional sum equal to ten percent (10%)

of such excess expenditure to cover the State's general expenses without the need to furnish proof in substantiation of such general expenses; or (iii) terminate this Contract for default, either in whole or in part by notice to Contractor (and without the need to afford Contractor any further opportunity to cure). Notwithstanding the foregoing, the State shall not use, as a basis for exercising its termination rights under this Section, deficiencies discovered in a repeat State Review Period that could reasonably have been discovered during a prior State Review Period.

The State, at any time and in its own discretion, may halt the UAT or approval process if such process reveals deficiencies in or problems with a Deliverable in a sufficient quantity or of a sufficient severity as to make the continuation of such process unproductive or unworkable. In such case, the State may return the applicable Deliverable to Contractor for correction and re-delivery prior to resuming the review or UAT process and, in that event, Contractor will correct the deficiencies in such Deliverable in accordance with the Contract, as the case may be.

Approval in writing of a Deliverable by the State shall be provisional; that is, such approval shall not preclude the State from later identifying deficiencies in, and declining to accept, a subsequent Deliverable based on or which incorporates or inter-operates with an approved Deliverable, to the extent that the results of subsequent review or testing indicate the existence of deficiencies in the subsequent Deliverable, or if the Application of which the subsequent Deliverable is a component otherwise fails to be accepted pursuant to **Section 2.080**.

2.254 PROCESS FOR APPROVAL OF WRITTEN DELIVERABLES

The State Review Period for Written Deliverables will be the number of days set forth in the applicable Statement of Work following delivery of the final version of the Written Deliverable (failing which the State Review Period, by default, shall be five (5) Business Days for Written Deliverables of one hundred (100) pages or less and ten (10) Business Days for Written Deliverables of more than one hundred (100) pages). The duration of the State Review Periods will be doubled if the State has not had an opportunity to review an interim draft of the Written Deliverable prior to its submission to the State. The State agrees to notify Contractor in writing by the end of the State Review Period either stating that the Written Deliverable is approved in the form delivered by Contractor or describing any deficiencies that shall be corrected prior to approval of the Written Deliverable (or at the State's election, subsequent to approval of the Written Deliverable). If the State delivers to Contractor a notice of deficiencies, Contractor will correct the described deficiencies and within five (5) Business Days resubmit the Deliverable in a form that shows all revisions made to the original version delivered to the State. Contractor's correction efforts will be made at no additional charge. Upon receipt of a corrected Written Deliverable from Contractor, the State will have a reasonable additional period of time, not to exceed the length of the original State Review Period, to review the corrected Written Deliverable to confirm that the identified deficiencies have been corrected.

2.255 PROCESS FOR APPROVAL OF CUSTOM SOFTWARE DELIVERABLES

The State will conduct UAT of each Custom Software Deliverable in accordance with the following procedures to determine whether it meets the criteria for State approval – i.e., whether it conforms to and performs in accordance with its specifications without material deficiencies.

Within thirty (30) days (or such other number of days as the parties may agree to in writing) prior to Contractor's delivery of any Custom Software Deliverable to the State for approval, Contractor shall provide to the State a set of proposed test plans, including test cases, scripts, data and expected outcomes, for the State's use (which the State may supplement in its own discretion) in conducting UAT of the Custom Software Deliverable. Contractor, upon request by the State, shall provide the State with reasonable assistance and support during the UAT process.

For the Custom Software Deliverables listed in an attachment, the State Review Period for conducting UAT will be as indicated in the attachment. For any other Custom Software Deliverables not listed in an attachment, the State Review Period shall be the number of days agreed in writing by the parties (failing which it shall be forty-five (45) days by default). The State Review Period for each Custom Software Deliverable will begin when Contractor has delivered the Custom Software Deliverable to the State

accompanied by the certification required by this **Section** and the State's inspection of the Deliverable has confirmed that all components of it have been delivered.

The State's UAT will consist of executing test scripts from the proposed testing submitted by Contractor, but may also include any additional testing deemed appropriate by the State. If the State determines during the UAT that the Custom Software Deliverable contains any deficiencies, the State will notify Contractor of the deficiency by making an entry in an incident reporting system available to both Contractor and the State. Contractor will modify promptly the Custom Software Deliverable to correct the reported deficiencies, conduct appropriate System Testing (including, where applicable, Regression Testing) to confirm the proper correction of the deficiencies and re-deliver the corrected version to the State for re-testing in UAT. Contractor will coordinate the re-delivery of corrected versions of Custom Software Deliverables with the State so as not to disrupt the State's UAT process. The State will promptly re-test the corrected version of the Software Deliverable after receiving it from Contractor.

Within three (3) business days after the end of the State Review Period, the State will give Contractor a written notice indicating the State's approval or rejection of the Custom Software Deliverable according to the criteria and process set out in this **Section**.

2.256 FINAL ACCEPTANCE

"Final Acceptance" shall be considered to occur when the Custom Software Deliverable to be delivered has been approved by the State and has been operating in production without any material deficiency for fourteen (14) consecutive days. If the State elects to defer putting a Custom Software Deliverable into live production for its own reasons, not based on concerns about outstanding material deficiencies in the Deliverable, the State shall nevertheless grant Final Acceptance of the Project.

2.260 Ownership

2.261 OWNERSHIP OF WORK PRODUCT BY STATE

Contractor grants to the State a royalty-free, nonexclusive, perpetual, unlimited and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use, for state government purposes, the software modifications, derivatives and improvements and associated documentation developed and/or obtained through this Contract or associated SOWs. Contractor and State understand and agree that these modifications will be included in the standard product and may be distributed to other customers.

2.262 VESTING OF RIGHTS

Intentionally left blank

2.263 RIGHTS IN DATA

The State is the owner of all data made available by the State to the Contractor or its agents, Subcontractors or representatives under the Contract. The Contractor will not use the State's data for any purpose other than providing the Services, nor will any part of the State's data be disclosed, sold, assigned, leased or otherwise disposed of to the general public or to specific third parties or commercially exploited by or on behalf of the Contractor. No employees of the Contractor, other than those on a strictly need-to-know basis, have access to the State's data. Contractor will not possess or assert any lien or other right against the State's data. Without limiting the generality of this Section, the Contractor must only use personally identifiable information as strictly necessary to provide the Services and must disclose the information only to its employees who have a strict need-to-know the information. The Contractor must comply at all times with all laws and regulations applicable to the personally identifiable information.

The State is the owner of all State-specific data under the Contract. The State may use the data provided by the Contractor for any purpose. The State will not possess or assert any lien or other right against the Contractor's data. Without limiting the generality of this Section, the State may use personally identifiable information only as strictly necessary to utilize the Services and must disclose the information only to its

employees who have a strict need to know the information, except as provided by law. The State must comply at all times with all laws and regulations applicable to the personally identifiable information. Other material developed and provided to the State remains the State's sole and exclusive property.

2.264 OWNERSHIP OF MATERIALS

The State and the Contractor will continue to own their respective proprietary technologies developed before entering into the Contract. Any hardware bought through the Contractor by the State, and paid for by the State, will be owned by the State. Any software licensed through the Contractor and sold to the State, will be licensed directly to the State.

2.270 State Standards

2.271 EXISTING TECHNOLOGY STANDARDS

The Contractor must adhere to all existing standards as described within the comprehensive listing of the State's existing technology standards at <http://www.michigan.gov/dmb/0,4568,7-150-56355-108233--.00.html>.

2.272 ACCEPTABLE USE POLICY

To the extent that Contractor has access to the State computer system, Contractor must comply with the State's Acceptable Use Policy, see http://michigan.gov/cybersecurity/0,1607,7-217-34395_34476---.00.html. All Contractor employees must be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State system. The State reserves the right to terminate Contractor's access to the State system if a violation occurs.

2.273 SYSTEMS CHANGES

Contractor is not responsible for and not authorized to make changes to any State systems without written authorization from the Project Manager. Any changes Contractor makes to State systems with the State's approval must be done according to applicable State procedures, including security, access and configuration management procedures.

2.274 ELECTRONIC RECEIPT PROCESSING STANDARD

All electronic commerce applications that allow for electronic receipt of credit/debit card and electronic check (ACH) transactions must be processed via the Centralized Electronic Payment Authorization System (CEPAS).

2.280 Extended Purchasing Program

2.281 EXTENDED PURCHASING PROGRAM

The Contract will be extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal. Upon mutual written agreement between the State of Michigan and the Contractor, this Contract may be extended to (a) State of Michigan employees, or (b) other states (including governmental subdivisions and authorized entities).

If extended, the Contractor must supply all goods and services at the established Agreement prices and terms. The State reserves the right to negotiate additional discounts based on any increased volume generated by such extensions.

The Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

2.290 Environmental Provision

2.291 ENVIRONMENTAL PROVISION

Energy Efficiency Purchasing Policy: The State seeks wherever possible to purchase energy efficient products. This includes giving preference to U.S. Environmental Protection Agency (EPA) certified 'Energy Star' products for any category of products for which EPA has established Energy Star certification. For other purchases, the State may include energy efficiency as one of the priority factors to consider when choosing among comparable products.

Environmental Purchasing Policy: The State of Michigan is committed to encouraging the use of products and services that impact the environment less than competing products. The State is accomplishing this by including environmental considerations in purchasing decisions, while remaining fiscally responsible, to promote practices that improve worker health, conserve natural resources, and prevent pollution. Environmental components that are to be considered include recycled content and recyclables; energy efficiency; and the presence of undesirable materials in the products, especially those toxic chemicals which are persistent and bioaccumulative. The Contractor should be able to supply products containing recycled and environmentally preferable materials that meet performance requirements and is encouraged to offer such products throughout the duration of this Contract. Information on any relevant third party certification (such as Green Seal, Energy Star, etc.) should also be provided.

Hazardous Materials: For the purposes of this Section, "Hazardous Materials" is a generic term used to describe asbestos, ACBMs, PCBs, petroleum products, construction materials including paint thinners, solvents, gasoline, oil, and any other material the manufacture, use, treatment, storage, transportation or disposal of which is regulated by the federal, state or local laws governing the protection of the public health, natural resources or the environment. This includes, but is not limited to, materials like as batteries and circuit packs, and other materials that are regulated as (1) "Hazardous Materials" under the Hazardous Materials Transportation Act, (2) "chemical hazards" under the Occupational Safety and Health Administration standards, (3) "chemical substances or mixtures" under the Toxic Substances Control Act, (4) "pesticides" under the Federal Insecticide Fungicide and Rodenticide Act, and (5) "hazardous wastes" as defined or listed under the Resource Conservation and Recovery Act.

- (a) The Contractor shall use, handle, store, dispose of, process, transport and transfer any material considered a Hazardous Material according to all federal, State and local laws. The State shall provide a safe and suitable environment for performance of Contractor's Work. Before the commencement of Work, the State shall advise the Contractor of the presence at the work site of any Hazardous Material to the extent that the State is aware of the Hazardous Material. If the Contractor encounters material reasonably believed to be a Hazardous Material and which may present a substantial danger, the Contractor shall immediately stop all affected Work, notify the State in writing about the conditions encountered, and take appropriate health and safety precautions.
- (b) Upon receipt of a written notice, the State will investigate the conditions. If (a) the material is a Hazardous Material that may present a substantial danger, and (b) the Hazardous Material was not brought to the site by the Contractor, or does not result in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Materials, the State shall order a suspension of Work in writing. The State shall proceed to have the Hazardous Material removed or rendered harmless. In the alternative, the State shall terminate the affected Work for the State's convenience.
- (c) Once the Hazardous Material has been removed or rendered harmless by the State, the Contractor shall resume Work as directed in writing by the State. Any determination by the Michigan Department of Community Health or the Michigan Department of Environmental Quality that the Hazardous Material has either been removed or rendered harmless is binding upon the State and Contractor for the purposes of resuming the Work. If any incident with Hazardous Material results in delay not reasonable anticipatable under the circumstances and which is attributable to the State,

the applicable SLAs for the affected Work will not be counted in a time as mutually agreed by the parties.

- (d) If the Hazardous Material was brought to the site by the Contractor, or results in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Material, or from any other act or omission within the control of the Contractor, the Contractor shall bear its proportionate share of the delay and costs involved in cleaning up the site and removing and rendering harmless the Hazardous Material according to Applicable Laws to the condition approved by applicable regulatory agency(ies).

Labeling: Michigan has a Consumer Products Rule pertaining to labeling of certain products containing volatile organic compounds. For specific details visit http://www.michigan.gov/deq/0,1607,7-135-3310_4108-173523--,00.html

Refrigeration and Air Conditioning: The Contractor shall comply with the applicable requirements of Sections 608 and 609 of the Clean Air Act (42 U.S.C. 7671g and 7671h) as each or both apply to this contract.

Environmental Performance: Waste Reduction Program - Contractor shall establish a program to promote cost-effective waste reduction in all operations and facilities covered by this contract. The Contractor's programs shall comply with applicable Federal, State, and local requirements, specifically including Section 6002 of the Resource Conservation and Recovery Act (42 U.S.C. 6962, et seq.).

2.300 Deliverables

2.301 SOFTWARE

A list of the items of software the State is required to purchase for executing the Contract is attached. The list includes all software required to complete the Contract and make the Deliverables operable. If any additional software is required in order for the Deliverables to meet the requirements of this Contract, such software shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Statement of Work or Contract Change Notice). The attachment also identifies certain items of software to be provided by the State.

2.302 HARDWARE

A list of the items of hardware the State is required to purchase for executing the Contract is attached. The list includes all hardware required to complete the Contract and make the Deliverables operable. If any additional hardware is required in order for the Deliverables to meet the requirements of this Contract, such hardware shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Contract Change Notice). The attachment also identifies certain items of hardware to be provided by the State.

2.310 Software Warranties

2.311 PERFORMANCE WARRANTY

The Contractor represents and warrants that Deliverables, after Final Acceptance, will perform and operate in compliance with the requirements and other standards of performance contained in this Contract (including all descriptions, specifications and drawings made a part of the Contract) for a period of (90) ninety days. In the event of a breach of this warranty, Contractor will promptly correct the affected Deliverable(s) at no charge to the State.

2.312 NO SURREPTITIOUS CODE WARRANTY

The Contractor represents and warrants that no copy of licensed Software provided to the State contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this Contract as the "No Surreptitious Code Warranty."

As used in this Contract, "Self-Help Code" means any back door, time bomb, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

As used in this Contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code. Unauthorized Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

In addition, Contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the State.

2.313 CALENDAR WARRANTY

The Contractor represents and warrants that all software for which the Contractor either sells or licenses to the State of Michigan and used by the State prior to, during or after the calendar year 2000, includes or shall include, at no added cost to the State, design and performance so the State shall not experience software abnormality and/or the generation of incorrect results from the software, due to date oriented processing, in the operation of the business of the State of Michigan.

The software design, to insure calendar year rollover compatibility, shall include, but is not limited to: data structures (databases, data files, etc.) that provide 4-digit date century; stored data that contain date century recognition, including, but not limited to, data stored in databases and hardware device internal system dates; calculations and program logic (e.g., sort algorithms, calendar generation, event recognition, and all processing actions that use or produce date values) that accommodates same century and multi-century formulas and date values; interfaces that supply data to and receive data from other systems or organizations that prevent non-compliant dates and data from entering any State system; user interfaces (i.e., screens, reports, etc.) that accurately show 4 digit years; and assurance that the year 2000 shall be correctly treated as a leap year within all calculation and calendar logic.

2.314 THIRD-PARTY SOFTWARE WARRANTY

The Contractor represents and warrants that it will disclose the use or incorporation of any third-party software into the Deliverables. At the time of Delivery, the Contractor shall provide in writing the name and use of any Third-party Software, including information regarding the Contractor's authorization to include and utilize such software. The notice shall include a copy of any ownership agreement or license that authorizes the Contractor to use the Third-party Software.

2.315 PHYSICAL MEDIA WARRANTY

Contractor represents and warrants that each licensed copy of the Software provided by the Contractor is free from physical defects in the media that tangibly embodies the copy. This warranty does not apply to defects discovered more than (30) thirty days after that date of Final Acceptance of the Software by the State. This warranty does not apply to defects arising from acts of Excusable Failure. If the Contractor breaches this warranty, then the State shall be entitled to replacement of the non-compliant copy by Contractor, at Contractor's expense (including shipping and handling).

2.320 Software Licensing

2.321 CROSS-LICENSE, DELIVERABLES ONLY, LICENSE TO CONTRACTOR

The State grants to the Contractor, the royalty-free, world-wide, non-exclusive right and license under any Deliverable now or in the future owned by the State, or with respect to which the State has a right to grant such rights or licenses, to the extent required by the Contractor to market the Deliverables and exercise its full rights in the Deliverables, including, without limitation, the right to make, use and sell products and services based on or incorporating such Deliverables.

2.322 CROSS-LICENSE, DELIVERABLES AND DERIVATIVE WORK, LICENSE TO CONTRACTOR

The State grants to the Contractor, the royalty-free, world-wide, non-exclusive right and license under any Deliverable and/or Derivative Work now or in the future owned by the State, or with respect to which the State has a right to grant such rights or licenses, to the extent required by the Contractor to market the Deliverables and/or Derivative Work and exercise its full rights in the Deliverables and/or Derivative Work, including, without limitation, the right to make, use and sell products and services based on or incorporating such Deliverables and/or Derivative Work.

2.323 LICENSE BACK TO THE STATE

Unless otherwise specifically agreed to by the State, before initiating the preparation of any Deliverable that is a Derivative of a preexisting work, the Contractor shall cause the State to have and obtain the irrevocable, nonexclusive, worldwide, royalty-free right and license to (1) use, execute, reproduce, display, perform, distribute internally or externally, sell copies of, and prepare Derivative Works based upon all preexisting works and Derivative Works thereof, and (2) authorize or sublicense others from time to time to do any or all of the foregoing.

2.324 LICENSE RETAINED BY CONTRACTOR

Contractor grants to the State a non-exclusive, royalty-free, site-wide, irrevocable, transferable license to use the Software and related documentation according to the terms and conditions of this Contract. For the purposes of this license, "site-wide" includes any State of Michigan office regardless of its physical location.

The State may modify the Software and may combine such with other programs or materials to form a derivative work. The State will own and hold all copyright, trademarks, patent and other intellectual property rights in any derivative work, excluding any rights or interest in Software other than those granted in this Contract.

The State may copy each item of Software to multiple hard drives or networks unless otherwise agreed by the parties.

The State will make and maintain no more than one archival copy of each item of Software, and each copy will contain all legends and notices and will be subject to the same conditions and restrictions as the original. The State may also make copies of the Software in the course of routine backups of hard drive(s) for the purpose of recovery of hard drive contents.

In the event that the Contractor shall, for any reason, cease to conduct business, or cease to support the Software, the State shall have the right to convert these licenses into perpetual licenses, with rights of quiet enjoyment, but subject to payment obligations not to exceed the then current rates.

2.325 PRE-EXISTING MATERIALS FOR CUSTOM SOFTWARE DELIVERABLES

All Intellectual Property Rights connected to the Contractor's pre-existing materials such as architectural structure, modules, and processes that may be used in the work, but do not constitute the whole of the finished work shall be owned by Contractor. The State shall own a royalty-free, irrevocable, perpetual use license for these architectural structures, modules, and processes that may be used in the work, as well as the whole of the finished works.

SOM shall retain all intellectual property rights in and to all client provided materials. Contractor disclaims any rights to or interest in any SOM provided materials (or any other assets or properties of SOM.)

2.330 Source Code Escrow

2.331 DEFINITION

"Source Code Escrow Package" shall mean:

- (a) A complete copy in machine-readable form of the source code and executable code of the Licensed Software, including any updates or new releases of the product;
- (b) A complete copy of any existing design documentation and user documentation, including any updates or revisions; and/or
- (c) Complete instructions for compiling and linking every part of the source code into executable code for purposes of enabling verification of the completeness of the source code as provided below. Such instructions shall include precise identification of all compilers, library packages, and linkers used to generate executable code.

2.332 DELIVERY OF SOURCE CODE INTO ESCROW

Contractor shall deliver a Source Code Escrow Package to the Escrow Agent, pursuant to the Escrow Contract, which shall be entered into on commercially reasonable terms subject to the provisions of this Contract within (30) thirty days of the execution of this Contract.

2.333 DELIVERY OF NEW SOURCE CODE INTO ESCROW

If at anytime during the term of this Contract, the Contractor provides a maintenance release or upgrade version of the Licensed Software, Contractor shall within ten (10) days deposit with the Escrow Agent, in accordance with the Escrow Contract, a Source Code Escrow Package for the maintenance release or upgrade version, and provide the State with notice of the delivery.

2.334 VERIFICATION

The State reserves the right at any time, but not more than once a year, either itself or through a third party contractor, upon thirty (30) days written notice, to seek verification of the Source Code Escrow Package.

2.335 ESCROW FEES

The Contractor will pay all fees and expenses charged by the Escrow Agent.

2.336 RELEASE EVENTS

The Source Code Escrow Package may be released from escrow to the State, temporarily or permanently, upon the occurrence of one or more of the following:

- (a) The Contractor becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for its business or assets, becomes subject to any proceeding under bankruptcy or insolvency law, whether domestic or foreign;
- (b) The Contractor has wound up or liquidated its business voluntarily or otherwise and the State has reason to believe that such events will cause the Contractor to fail to meet its warranties and maintenance obligations in the foreseeable future;
- (c) The Contractor voluntarily or otherwise discontinues support of the provided products or fails to support the products in accordance with its maintenance obligations and warranties.

2.337 RELEASE EVENT PROCEDURES

If the State desires to obtain the Source Code Escrow Package from the Escrow Agent upon the occurrence of an Event in this **Section**, then:

- (a) The State shall comply with all procedures in the Escrow Contract;
- (b) The State shall maintain all materials and information comprising the Source Code Escrow Package in confidence in accordance with this Contract;

- (c) If the release is a temporary one, then the State shall promptly return all released materials to Contractor when the circumstances leading to the release are no longer in effect.

2.338 LICENSE

Upon release from the Escrow Agent pursuant to an event described in this **Section**, the Contractor automatically grants the State a non-exclusive, irrevocable license to use, reproduce, modify, maintain, support, update, have made, and create Derivative Works. Further, the State shall have the right to use the Source Code Escrow Package in order to maintain and support the Licensed Software so that it can be used by the State as set forth in this Contract.

2.339 DERIVATIVE WORKS

Any Derivative Works to the source code released from escrow that are made by or on behalf of the State shall be the sole property of the State. The State acknowledges that its ownership rights are limited solely to the Derivative Works and do not include any ownership rights in the underlying source code.

Glossary

Days	Means calendar days unless otherwise specified.
24x7x365	Means 24 hours a day, seven days a week, and 365 days a year (including the 366th day in a leap year).
Additional Service	Means any Services/Deliverables within the scope of the Contract, but not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
Audit Period	See Section 2.110
Business Day	Whether capitalized or not, shall mean any day other than a Saturday, Sunday or State-recognized legal holiday (as identified in the Collective Bargaining Agreement for State employees) from 8:00am EST through 5:00pm EST unless otherwise stated.
Blanket Purchase Order	An alternate term for Contract as used in the States computer system.
Business Critical	Any function identified in any Statement of Work as Business Critical.
Chronic Failure	Defined in any applicable Service Level Agreements.
Deliverable	Physical goods and/or commodities as required or identified by a Statement of Work
DTMB	Michigan Department of Technology, Management and Budget
Environmentally preferable products	A product or service that has a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. Such products or services may include, but are not limited to, those that contain recycled content, minimize waste, conserve energy or water, and reduce the amount of toxics either disposed of or consumed.
Excusable Failure	See Section 2.244.
Hazardous material	Any material defined as hazardous under the latest version of federal Emergency Planning and Community Right-to-Know Act of 1986 (including revisions adopted during the term of the Contract).
Incident	Any interruption in Services.
ITB	A generic term used to describe an Invitation to Bid. The ITB serves as the document for transmitting the RFP to potential bidders
Key Personnel	Any Personnel designated in Article 1 as Key Personnel.
New Work	Any Services/Deliverables outside the scope of the Contract and not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
Ozone-depleting substance	Any substance the Environmental Protection Agency designates in 40 CFR part 82 as: (1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or (2) Class II, including, but not limited to, hydro chlorofluorocarbons
Post-Consumer Waste	Any product generated by a business or consumer which has served its intended end use, and which has been separated or diverted from solid waste for the purpose of recycling into a usable commodity or product, and which does not include post-industrial waste.
Post-Industrial Waste	Industrial by-products that would otherwise go to disposal and wastes generated after completion of a manufacturing process, but do not include internally generated scrap commonly returned to industrial or manufacturing processes.
Recycling	The series of activities by which materials that are no longer useful to the generator are collected, sorted, processed, and converted into raw materials and used in the production of new products. This definition excludes the use of these materials as a fuel substitute or for energy production.
Reuse	Using a product or component of municipal solid waste in its original form more than once.
RFP	Request for Proposal designed to solicit proposals for services
Services	Any function performed for the benefit of the State.
Source reduction	Any practice that reduces the amount of any hazardous substance, pollutant, or

	contaminant entering any waste stream or otherwise released into the environment prior to recycling, energy recovery, treatment, or disposal.
State Location	Any physical location where the State performs work. State Location may include state-owned, leased, or rented space.
Subcontractor	A company Contractor delegates performance of a portion of the Services to, but does not include independent contractors engaged by Contractor solely in a staff augmentation role.
Unauthorized Removal	Contractor's removal of Key Personnel without the prior written consent of the State.
Waste prevention	Source reduction and reuse, but not recycling.
Waste reduction and Pollution prevention	The practice of minimizing the generation of waste at the source and, when wastes cannot be prevented, utilizing environmentally sound on-site or off-site reuse and recycling. The term includes equipment or technology modifications, process or procedure modifications, product reformulation or redesign, and raw material substitutions. Waste treatment, control, management, and disposal are not considered pollution prevention, per the definitions under Part 143, Waste Minimization, of the Natural Resources and Environmental Protection Act (NREPA), 1994 PA 451, as amended.
Work in Progress	A Deliverable that has been partially prepared, but has not been presented to the State for Approval.
Work Product	Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Contractor as a result of an in furtherance of performing the services required by this Contract.

Attachment 1 – Service Level Agreement

PERPETUAL USE LICENSE, IMAGETREND HOSTED SOLUTION VERSION 3.0

This agreement exists for the purpose of creating an understanding between ImageTrend and CLIENT who elect to host the application on ImageTrend's servers. It is part of our guarantee for exceptional service levels for as long as the system annual support fee is contracted. The Licensed ImageTrend Hosted Solution Service Level Agreement guarantees your web application's availability, reliability and performance. This Service Level Agreement (SLA) applies to any site or application hosted on our network as contracted.

1. Hosting at the ImageTrend's Datacenter

ImageTrend's hosting environment provides **99.9% availability** and is comprised of state-of-the-art Blade Servers and SAN storage that are configured with the no single point of failure through software and infrastructure virtualization, blade enclosure redundancies and backup storage policies. Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN. Scheduled maintenance and upgrades do not apply to the system availability calculation and all CLIENTs are properly notified of such scheduled occurrences to minimize accessibility interruptions.

Hardware

ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
 - Microsoft SQL Server 2012
 - Microsoft Windows Server 2008
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Disk Space allocation and Bandwidth as contracted

Physical Facility

The ImageTrend hosting facility is located in downtown Minneapolis with every industry standard requirement for hosting not only being met, but exceeded. Requirements such as power supply and power conditioning, normal and peak bandwidth capacity, security and fail over locations are all part of an overall strategy to provide the most reliable hosting facility possible.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression
- Secured site access

- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity

ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.
- Daily Scheduled backup Success/Failure notification via cell-phone and email

2. Application and Hosting Support

ImageTrend provides ongoing support as contracted for their applications and hosting services, including infrastructure. This includes continued attention to product performance and general maintenance needed to ensure application availability. Support includes technical diagnosis and fixes of technology issues involving ImageTrend software. ImageTrend has a broad range of technical support services available in the areas of:

- Web Application Hosting and Support
- Subject Matter Expert Application Usage Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

ImageTrend offers multi-level technical support, based on level-two user support by accommodating both the general inquiries of the administrators and those of the system users. We will give the administrators the ability to field support for the system as the first level of contact while providing them the option to refer inquiries directly to ImageTrend.

ImageTrend's Support Team is available 24/7 at support@imagetrend.com and www.imagetrend.com/support as well as Monday through Friday from 8:00 am to 5:30 pm CST at:

Toll Free: 1-888-730-3255
Phone: 952-469-1589

Online Support Desk

ImageTrend offers an online support system, Support Desk, which incorporates around-the-clock incident reporting of all submitted tickets to ImageTrend's support desk specialists. Once a client submits a support ticket, he or she can easily track its process with a secure login, promoting a support log for the client and ImageTrend's support team. The system promotes speedy resolution by offering keyword-based self-help services and articles in the knowledgebase, should clients wish to bypass traditional support services. Ticket tracking further enhances the efforts of Support Desk personnel by allowing them to identify patterns which can then be utilized for improvements in production, documentation, education and frequently asked questions to populate the knowledgebase. The support ticket tracking system ensures efficient workflow for the support desk specialists while keeping users informed of their incident's status. Support patterns can be referenced to populate additional knowledgebase articles.

Incident Reporting Malfunctions

ImageTrend takes all efforts to correct malfunctions that are documented and reported by the Client. ImageTrend acknowledges receipt of a malfunction report from a Client and acknowledges the disposition and possible resolution thereof according to the chart below.

Severity Level	Examples of each Severity Level:	Notification Acknowledgement: ImageTrend Return Call to Licensee after initial notification of an Error	Action Expectation: Anticipated Error resolution notification after ImageTrend Return Call to Licensee of Notification Acknowledgement of an error.
Severity 1 – Critical	<ul style="list-style-type: none">- Complete shutdown or partial shutdown of one or more Software functions- Access to one or more Software functions not available- Major subset of Software application impacted	Within one (1) hour of initial notification during business hours or via support@imagnetrend.com or Support Desk with critical subject status.	Six hours
Severity 2 – Non-Critical	<ul style="list-style-type: none">- Minor subsystem failure-Data entry or access impaired on a limited basis – usually can be delegated to local client contact as a first level or response for resolution – usually user error (i.e. training) or forgotten passwords	Within four (4) hours of initial notification	24 Business hours
Severity 3 – Non-essential	<ul style="list-style-type: none">- System operational with minor issues; suggested enhancements as mutually agreed upon – typically covered in next version release as mutually agreed upon.	Same day or next business day of initial notification	Next Release

Service Requests (enhancements)

Any service requests that are deemed to be product enhancements are detailed and presented to the development staff, where the assessment is made as to whether these should be added to the future product releases and with a priority rating. If an enhancement request is specific to one client and deemed to be outside of the original scope of the product, then a change order is written and presented to the Client. These requests are subject to our standard rates and mutual agreement. Clients review and approve the scope, specification and cost before work is started to ensure goals are properly communicated.

Product release management is handled by ImageTrend using standard development tools and methodologies. Work items including, tasks, issues, and scenarios are all captured within the system. Releases are based on one or more iterations during a schedule development phase. This includes by not limited to: development, architecture, testing, documentation, builds, test and uses cases. Submissions of issues or requests are documented within our Product Management system and from there workflow is created to track the path from initial request to resolution.

Out of Scope

Client may contract with ImageTrend for Out of Scope services. This will require a separate Statement of Work and will be billed at ImageTrend’s standard hourly rate.

Maintenance and Upgrades

System/product maintenance and upgrades, if applicable, are included in the ongoing support and warranty as contracted. These ensure continued attention to product performance and general maintenance. Scheduled product upgrades include enhancements and minor and major product changes. Customers are notified in advance of scheduled maintenance. It is the Client's responsibility to accept all offered updates and upgrades to the system. If the Client does not accept these, Client should be advised that ImageTrend, at its discretion, may offer limited support for previous versions. All code releases also maintain the integrity of any client specific configurations (i.e. templates, addresses, staff information, active protocols, etc.) that have been implemented either by ImageTrend's implementation staff or the client's administrative staff.

Escalation

Our support staff is committed to resolving your issues as fast as possible. If they cannot resolve your issue immediately, they will identify the course of action that they will be taking and indicate when an answer will be available. They in turn will seek assistance from the designated developer. The next level of escalation goes to the Project Manager, who also addresses all operational issues on an ongoing basis and reviews the issue log regularly to assess product performance and service levels. Senior Management will handle issues requiring further discussion and resolution. Any issues to be determined to be of a critical nature are immediately brought to the attention of both the X-Team and Senior Management.

Attachment 2 – Hosting Environment

Web/Application Server

Dual Quad Core Processors
32 GB RAM
SAN Data Storage
Blade Servers with Microsoft Hyper-V

Operating Systems

Microsoft Windows 2008 R2 Server

Web Server Software

Microsoft IIS version 7.0 or later

Addition Service Software

Microsoft .NET Framework 2.0, 3.5 SP1 and 4.0
Microsoft Tablet PC SDK

Additional Application Software

Adobe ColdFusion 9 Enterprise

Database Server (Separate database servers)

Hardware

Dual Quad Core Processors
8-16 GB RAM
100 GB Available Hard Disk Space
100,000 + incidents per year: 200 GB
RAID 5 SCSI Hard Drives

Software (64-bit recommended)

Microsoft SQL Server 2012

Internet Browser Requirements for End Users

Microsoft Internet Explorer 8.0 and above
Other browsers that support Mozilla 4.0 and above
Adobe Reader 10 or higher
Adobe Flash 11 or higher (recommended)
Microsoft Silverlight 2.0 (recommended)

Minimum Requirements for End Users using the DRF (Dynamic Run Form)

Software
Microsoft Silverlight 3.0

Hardware

OS: Windows XP SP2
RAM: 1GB
Processor: 1.2 GHz

Network

64 kbps ISDN/DSL (Cable or DSL)

ImageTrend Hosting

Integral to any online solution is a quality data center providing application access, availability, data security and overall confidence. ImageTrend's facilities incorporate industry leading infrastructure, application security and excellent technical support for our hosted solutions. ImageTrend offers experience and the latest technology for our hosted applications. To date over 60,000,000 incidents have been documented and stored utilizing ImageTrend Bridge products. Another benefit to an ImageTrend hosted solution is the long-term cost savings to the client in hardware investments and maintenance and the staff levels and commitment to maintaining a datacenter that is secure and reliable for HIPAA data storage.

System Upgrades/Updates

As a system hosted by ImageTrend, we manage all aspects of the software installation and server infrastructure. Any upgrades are applied following a release schedule, which includes prior notification of the availability of the upgrade, the anticipated scheduled maintenance and allowing for sufficient time to accommodate any client concerns or constraints. Our virtual infrastructure supports many types of upgrades or fixes to be applied without any system downtime and therefore unnoticed by a client. Updates to the Field Bridge are administrated through the Service Bridge. The system administrator can determine when to push the updates to the Field Bridge. The update is then installed by Windows restricted users. The Field Bridge user will get a message at login indicating that an update is available. They can choose to install or cancel. The user does not have to be an administrator to run an update.

If the application is hosted by the client, our staff notifies the client's staff that an upgrade is available with recommendations for installation. We may assist in this provided we are given a VPN and system access.

License Options

Over 70% of ImageTrend's solutions are hosted at ImageTrend's data center. Any of those solutions hosted with ImageTrend may have the solution's licensure offered as a one-time purchase or it can be included in the monthly hosting fees, which ImageTrend defines as Software as a Service (SaaS) – application usage lease, support and hosting in one annual fee. All solutions provided by ImageTrend can alternatively be hosted at the client's data center.

Availability

ImageTrend's hosting environment provides 99.9% availability and is comprised of state-of-the-art Blade Servers and SAN storage that ensure this with software and infrastructure virtualizations, blade computing redundancies and backup storage policies. Our data center service is recognized by Microsoft as being in the top 100 of their "Top Tiered Hosting Partners". If 99.99% availability is desired, which includes our second data center in Chicago, additional hosting costs will apply.

Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN.

Data Retention

Information will be stored in the system for as long as desired by the client. Archived information will still be accessible by the System Administrators. Data will only be purged upon a client request.

Hardware

ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
 - Microsoft SQL Server 2012
 - Microsoft Windows Server 2008 R2
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Weekly, monthly or quarterly backups (as contracted)
- Periodic CD-ROM backups (as contracted)
 - Weekly, monthly or quarterly
 - Offsite vaulting and escrow
- 30 GB Disk Space allocation per month with additional space in 10 GB increments
- 3 Mb Traffic or Bandwidth per month with additional bandwidth available in 1 Mb increments

Physical Facility

The ImageTrend hosting facility is located in downtown Minneapolis with every industry standard requirement for hosting not only being met, but exceeded. Requirements such as power supply and power conditioning, normal and peak bandwidth capacity, security and fail over locations are all part of an overall strategy to provide the most reliable hosting facility possible.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression
- Secured site access
- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity

ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.
- Daily Scheduled backup Success/Failure notification via cell-phone and email

Support Services

ImageTrend provides both onsite and on-call support for their applications and hosting.

Support includes technical diagnosis and fixes of technology issues involving software and hardware. ImageTrend has a broad range of technical support to their systems and proposes to provide service in the areas of:

- Web Site Hosting and Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

Phone support is available Monday through Friday from 7:00 AM - 6:00 PM CST.

ImageTrend also provides onsite resolution for support of their applications either at their location in Lakeville, MN or at the client's location as the situation dictates.

Attachment 3 – ImageTrend Security and Disaster Recovery Process

ImageTrend has included information describing the security for the IT environment in this section of our response, as well as our Disaster Recovery Plan. The EDS Data Security Policies and Procedures document has been included in Attachment 4.

Security

ImageTrend applications meet or exceed State and federal data privacy requirements and the HIPAA guidelines. Secure logins are an industry standard process and are part of the HIPAA guidelines for data protection. These are implemented throughout the application with the use of the hierarchical security access features of the ImageTrend security module, which provides the environment for controlling the access necessary to provide data protection. The application also provides for security breach notifications and audit trails.

Application Securities

Secure User Login

- The application adheres to business standard practices for security to ensure only authorized access to the system

Password Encryption

- Hash function implementation
- Temporary account suspension for sessions failing to successfully login after three tries
- Check access log for sequential unsuccessful logins
- Set session logout variable

Password Requirements

- Length and Complexity Enforcement
- Validate Password for Case, Length (8 characters), and Composition

Login Expirations

- Validate for expired logins
- Force password changes on expired logins and restrict site access until new, valid password is created

Page Access Checking

- Page Access Checking to make sure user has properly logged in and is not entering the site via an external link

SSL Server Certificate

- 128-bit encryption Security Certificate

Permissions Administration

Manage Users and Groups

The application employs a hierarchical based password administration as a series of group policies to control application entry and level of access within the application. With the system administrator being the highest level of security, groups can be created below that to encompass all other group needs, which may include:

- Director – Access to view all runs within their service.
- Multiple Service Administrators – User Access and administration to multiple services.

Permissions and Rights

Permission and rights are governed by the ability of what the user can see and do. At the global level, rights are based on the following criteria:

- County
- City
- Service

On the service level, there are two levels:

- Administrator
- User

Service administrators can control and edit all the functions with their own service. Service users have the ability to edit and view their own information.

Password Administration

Through the Application Access Control, the system administrator can determine several features regarding the password administration:

- Number of days without login to the application before the user's account is suspended
- Number of attempts a user can attempt to login before their account is placed on temporary suspend
- Set the password to contain at least one numeric character
- Set the password to contain at least one uppercase character
- Time in hours that a user cannot change their password after last change
- Number of past passwords stored in the log table for a user
- Number of passwords in the log table to be compared with the newest password to prevent repeat use of passwords
- Minimum number of characters in the password
- Number of days the user will be notified before they must change their password
- An Email Confidentiality statement can be added, edited and deleted
- An inactive account message can be added, edited and deleted
- Security questions prompt on login or password retrieval
- Encrypt security question answer

Procedural Securities

Hosting Environment

ImageTrend's Web applications are hosted in our state-of-the-art, 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically and a log book is kept to monitor and record individuals accessing the server room.

ImageTrend's production network consists of application/web and database servers. The databases are on a private network with access control managed through the firewall, permitting only authorized administrators or approved VPN access.

Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation trigger email alerts which are sent to support staff and cell phone alerts to ImageTrend's 24/7 X-Team Support staff. Our X-Team support employees have VPN access to our production servers, to ensure accessibility and security, when accessing our servers from outside of our network

Auditing

The Service Bridge's audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database. This database is kept for a period of time for reporting purposes and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosures. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

Personnel

All ImageTrend employees are subjected to background checks and are required to attend and successfully complete HIPAA training. The ImageTrend Project Management System gives us a facility to track any HIPAA Security Incidents or Information Disclosure Incidents for reporting purposes.

Only those certified ImageTrend employees that work with either hardware or software related to the specified application or project will access the data center and interact with our servers. These employees have worked with our hardware as part of our IT support staff or are part of our Implementation team as software developers. Authorization is granted from the management level.

Disaster Recovery

ImageTrend, Inc. follows a specific critical path for organizations and companies during a recovery effort, to ensure the resumption of normal operations in the event of a disaster. This process has seven stages, which are followed regardless of the organization. In a disaster recovery plan it is important to minimize the loss of data and return application usage as quickly as possible.

Stage 1 - Immediate Response

The first step in the recovery process and the initial reaction to a potential disaster or interruption consists of immediate assessment and if necessary, notification of clients of interruption and any actions they should undertake. In many situations the system's redundancies will accommodate the situation and provide continuity. This takes place within the first 4 hours.

Stage 2 - Environment Restoration

The necessary steps for restoring service via repairs or alternate infrastructure are begun by gathering the necessary components for restoration and installing. If local repair is not possible due to extreme conditions, then the service will be redirected to another data center and the required DNS redirection may take up to 8 hours to propagate.

Stage 3 - Functional Restoration

Application functionality is tested on restored or alternate service site to ensure user access and usability. For same data center restoration within 8 hours and for alternate site usage within 24 hours.

Stage 4 - Data Restoration and Synchronization

This step includes backlog reduction. Data from offsite locations is restored to the restored environment. Database backups are automatically done every 2 hours, daily and weekly. These backups will be used for data restoration and synchronization. Maximum data window will be two hours. Most often, data is protected at different times during the business cycle and must be reconstructed or synchronized before it can be used. Synchronizing, validating, and reviewing data from many different sources is a critical step in a successful recovery. Once reliable data is established, backlogged transactions that have accumulated during recovery can be processed. This may take up to 48 hours, however application usage is available during this time.

Stage 5 - Business Resumption

Clients will be notified that the affected service can now resume its normal operations.

Stage 6 - Interim Site Migration

Once the primary site environment has been restored, return migration is planned and scheduled. Depending on the nature of the problem, this may take an extended period of time to restore the environment. Disruption of services during this transition will be minimized and clients will be notified of the impact and a schedule of return will be mutually discussed.

Stage 7 - Return to Home Site

All recovery efforts have been completed, and a business may resume normal operations at its primary location.

Backups

Code Backups

Application code is backed up daily; at least a daily backup exists for all applications hosted in ImageTrend's production environment and is included in hosting costs. These backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. Daily backups are retained for longer as unallocated storage permits but not guaranteed to be available beyond the previous calendar day. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Database Backups

Database files are backed up daily; at least a daily backup exists for any database hosted in ImageTrend's production environment and is included in hosting costs. Daily backups are retained for several days as unallocated storage permits but not guaranteed to be available beyond three previous calendar days. Database backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Restore Procedures

Daily backup files are stored uncompressed to facilitate quick recovery of one or more files as needed. Archive copies are compressed to conserve disk space. All database files are compressed to conserve disk space and must be uncompressed and reattached for restoration. When restoring a file the newer file, if it exists, is renamed and kept before replacing with the backup version. When restoring an entire database file, the copy being replaced is itself backed up before being modified. When restoring part of a database file, the current file is first backed up and the backup database is mounted with a different name, then the needed tables are restored and the backup file is detached. If restoring a complete backup of application code over a corrupted install, a copy of the bad files is kept to maintain any new user-added files since the backup was created.

Attachment 4 – EDS Data Security Policies and Procedures

DATA SECURITY POLICY OVERVIEW

This document defines the data security policy of ImageTrend, Inc. ImageTrend, Inc. takes the privacy of our employees and clients very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.

Intent

The goal of this policy is to inform ImageTrend employees and customers of the rules and procedures relating to data security compliance.

The ImageTrend data covered by this policy includes, but is not limited to all electronic information found in e-mail, databases, applications and other media; paper information, such as hard copies of electronic data, employee files, internal memos, and so on.

The Client data covered by this policy includes, but is not limited to all electronic information collected by any ImageTrend software application, which is hosted at the ImageTrend data center.

Audience

This policy applies to all employees, management, contractors, vendors, business partners and any other parties who have access to company and/or client data.

Data Types

ImageTrend, Inc. deals with two main kinds of data:

1. **Company-owned data** that relates to such areas as corporate financials, employment records, payroll, etc.
2. **Private data** that is the property of our clients and/or employees, such as social security numbers, credit card information, contact information, patient data, etc.

Data Classifications

ImageTrend, Inc.'s data is comprised of 3 classifications of information:

1. **Public/Unclassified.** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials, and other data as applicable.

Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. **Private.** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies, and other data as applicable.

All information not otherwise classified will be assumed to be Private.

Employees may not disclose private data to anyone who is not a current employee of the company.

3. **Confidential.** This is defined as personal or corporate information that may be

considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as

applicable]. ImageTrend, Inc. considers it a top priority to protect the privacy of our clients and employees

Employees may only share confidential data within the department or named distribution list and with proper authorization.

4. **Secret/Restricted.** This is defined as sensitive data which, if leaked, would be harmful to ImageTrend, Inc., its employees, contractors, and clients. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes but is not limited to audit reports, legal documentation, business strategy details, patient data, and other data as applicable.

Secret/restricted data cannot be disclosed by anyone other than the original author, owner or distributor.

It is the responsibility of everyone who works at ImageTrend, Inc. to protect our own and client data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

Responsibilities

All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.

Management is responsible for ensuring that their direct reports understand the scope and implications of this policy. HR must also ensure that all employees attend data privacy training and have evidence thereof and a signed copy of this policy in their file.

Security staff will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.

Any employee who authors or generates corporate or client data must classify that data according to the criteria outlined above.

Management

Ownership of this policy falls to Security Officer. For any questions about this policy, or to report misuse of corporate or personal data, please contact him/her at (952) 469-1589. The IT department will work in conjunction with the client to maintain data access privileges, which will be updated as required when an employee joins or leaves the company. These are the accepted technologies ImageTrend, Inc. used to enforce and ensure data security:

1. Access controls
2. Strong passwords
3. System monitoring
4. Personnel Training

Review

Management is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

On an annual basis, unless previous action was required, we review our security policies and procedures to ensure that necessary updates have occurred. We welcome any security reviews that our customers might request at their expense. Several clients have performed such reviews over the years and have been satisfied with the results.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPLICATION SECURITY

DATA WAREHOUSE SECURITY

EMS State Bridge/EMS Service Bridge/Rescue Bridge

The ImageTrend applications meet or exceed State and federal data privacy requirements and the HIPAA guidelines. Secure logins are an industry standard process and are part of the HIPAA guidelines for data protection. These are implemented throughout the application with the use of the multi-tiered hierarchical security access features of the ImageTrend security module, which provides the environment for controlling the access necessary to provide data protection.

The reporting and auditing functions of the application's procedures allow for safeguarding and immediate notifications of any attempted breaches. This provides for data access only through assigned permissions and ensures that only those intended see their data and can access it for reporting.

Application Securities

- Secure User Login
- Password Encryption
- Password Requirements
- Login Expirations
- Page Access Checking
- SSL Server Certificate: 128-bit encryption Security Certificate
- CAD data sent using secure Web Service

Permissions Administration

Manage Users and Groups

The application employs a hierarchical based password administration as a series of group policies to control application entry and level of access within the application. With the system administrator being the highest level of security, groups can be created below that to encompass all other group needs, which may include:

- Director – Access to view all runs within their service.
- Multiple Service Administrators – User Access and administration to multiple services.

Permissions and Rights

Permission and rights are governed by the ability of what the user can see and do. At the global level, rights are based on the following criteria:

- County
- City
- Service

On the service level, there are two levels:

- Administrator
- User

Service administrators can control and edit all the functions with their own service. Service users have the ability to edit and view their own information.

Password Administration

Through the Application Access Control, the system administrator can determine several features regarding the password administration:

- Number of days without login to the application before the user's account is suspended
- Number of attempts a user can attempt to login before their account is placed on temporary suspend
- Set the password to contain at least one numeric character
- Set the pass word to contain at least one uppercase character
- Number of past passwords stored in the log table for a user
- Number of passwords in the log table to be compared with the newest password to prevent repeat use of passwords
- Minimum number of characters in the password
- Number of days the user will be notified before they must change their password
- An Email Confidentiality statement can be added, edited and deleted
- An inactive account message can be added, edited and deleted
- Security questions prompt on login or password retrieval
- Encrypt security question answer

Procedural Securities

Hosting Environment

ImageTrend's Web applications are hosted in our state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book is kept to monitor and record individuals accessing the server room.

ImageTrend's production network consists of application/web and database servers. The databases are on a private network with access control managed through the firewall permitting only authorized administrators or approved VPN access.

Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation trigger email alerts which are sent to support staff and cell phone alerts to ImageTrend's 24/7 X-Team Support staff. Our X-Team support employees have VPN access to our production servers, to ensure accessibility and security, when accessing our servers from outside of our network.

Auditing

The system's audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database, which is kept for a period of time for reporting purpose and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosers. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

FIELD COLLECTION SECURITY

EMS Field Bridge

Security for Field Bridge conforms to the current best practices and new technology. Security enhancements have been performed both behind the scenes with increased database security and through settings that administrators can configure for automatic run removal and password requirements.

Data Storage Security

Data storage for each Field Bridge works with Microsoft SQL CE 2008. This software provides greater data security for all patient data. The databases contained within SQL CE 2008 are password protected to prevent unauthorized access and the entire database is completely encrypted with 128-bit encryption. In addition, all patient data within the database is further encrypted using Rijndael (AES) cipher algorithm using a 128-bit key and IV, assemblies are obfuscated and string encrypted. Data received through a CAD integration is sent via secure Web Services.

Data Sync to Service/Rescue/State Bridge

The ImageTrend EMS Field Bridge complies with W3C web Service and XML standards. Data is synced from the Field Bridge to the Service/Rescue/State Bridge through secure web service communication utilizing 128-bit SSL Certificate which encrypts all data during transmission.

There are three authentication parameters that are required to be sent with the web service request as outlined below. A user account will be set up within the Field Bridge system to track access and assign any actions to a particular user. An additional API token will be created for web service authentication.

- token=uniqueidentifier
- userID=string
- password=string

Administrative-Set Security Options

Administrators have the ability to configure the Field Bridge to provide additional security. Additional security is possible based on your service's IT departments and policies.

Clearing Out Old Incidents

Administrators can choose to delete old incidents from the Field Bridge database after a certain number of days and after those incident reports have been posted to the Service Bridge, State Bridge or Rescue Bridge system working with this Field Bridge. Automatically removing old incidents will reduce the amount of patient data available in the system at any one time without causing any additional time to manually clean out the database, reducing any risk of a security issue.

Usernames and Passwords

Within the Field Bridge, any user who wants to work with the application must log in with a username and password set up on the Service Bridge, State Bridge or Rescue Bridge to which this Field Bridge is assigned. Administrators can set up the password requirements, the length of time in between required password changes and any restrictions on the user's access to portions of the Field Bridge.

HOSTING OVERVIEW

ImageTrend's hosting environment provides 99.9% availability and is comprised of state-of-the-art Blade Servers and SAN storage that ensure this with software and infrastructure virtualizations, blade computing redundancies and backup storage policies. Our data center service is recognized by Microsoft as being in the top 100 of their "Top Tiered Hosting Partners".

Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN. Information will be stored in the system for as long as desired by the client. Archived information will still be accessible by the System Administrators. Data will only be purged upon a client request.

Hardware

ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
 - Microsoft SQL Server 2012
 - Microsoft Windows Server 2008
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Weekly, monthly or quarterly backups (as contracted)
- Periodic CD-ROM backups (as contracted)
 - Weekly, monthly or quarterly
 - Offsite vaulting and escrow
- 30 GB Disk Space allocation per month with additional space in 10 GB increments
- 3 Mb Traffic or Bandwidth per month with additional bandwidth available in 1 Mb increments

Physical Facility

ImageTrend's Web applications are hosted in our state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book is kept to monitor and record individuals accessing the server room.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression
- Secured site access
- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity

ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.
- Daily Scheduled backup Success/Failure notification via cell-phone and email

SERVER MONITORING

This section outlines the process followed to ensure server stability and proactively reduce server incidents.

Server Status

All ImageTrend production servers are monitored 24/7 for system health and service availability. Status information includes:

- current users accessing the system
- disk use
- memory use
- CPU use
- Notification of hardware failures

Server logs are kept on a separate server and are available for review even in the event that a server fails for forensic use in determining the state shortly before a problem occurred. Server status is recorded and any dramatic change in a metric generates an alert message to all available support staff.

Application Status

All ImageTrend production servers are monitored 24/7 for the status of Web services and ImageTrend applications. Status information includes:

- application availability
- application response time
- failure status codes

A change in application status generates an alert message to all available support staff. General application responsiveness is tested, not individual client sites are monitored, so an error in a single application may go undetected by this system.

Monitoring Intervals and Response Times

Monitoring events occur between every three and eight minutes depending on the application and server being monitored. Monitoring takes place from multiple locations with staggered start times resulting in a monitoring resolution of approximately two to five minutes. Alerts generated by the monitoring system are sent to support staff via email and SMS to cell phones, with an average transmission time of one minute.

SERVER INCIDENT RESPONSE

Service Recycling

The most common cause of service unavailability is a failed service. A failed service is given 10 minutes to recycle or the problem is escalated to a server restart. Other action may be taken as the situation warrants, given service specific errors or an obvious cause for the failure.

Server Restart

A server restart should be undertaken if a service recycling does not solve the failure or further troubleshooting. Normal operating system functions for restarting should be used if possible. Otherwise using ImageTrend's remote controllable power outlets the server should be cold booted. The progress of the restart is observed using ImageTrend's IP enable KVM switch allowing BIOS or other hardware errors to be observed and worked through.

Transferring Websites

If within 50 minutes of the initial alert being issued services have not been restored and a solution does not appear to be immediately forthcoming, the services and roles of the unavailable server will be moved to an alternate location. ImageTrend maintains an extra server capacity to allow for this flexibility with minimal disruption to other services. If the original files are unavailable backups will be used to recreate the original server configuration. As the same IP addresses are used to restore service no DNS changes are required and the restoration is immediate. While in transition the websites affected will display a message describing the problem and an estimation of the time to service being restored.

Transferring Locations

If service cannot be restored by transferring to a different server within the same environment, services will be moved to an alternate hosting location. A backup datacenter is available in Chicago, IL, for hosting mission critical applications. Code and database backups are pushed to this location to be used in the event of disaster which disables the primary datacenter in Minneapolis, MN. Clients requiring automatic failover can opt for DNS failover which detects service unavailability and automatically moves DNS records to refer to the backup location. Other clients will be moved to the backup datacenter as needed and DNS changes will be made manually or requested immediately upon the initiation of relocation.

Hardware Replacement

Whenever a hardware failure contributes to a server failure the hardware in question will be replaced aggressively before redeploying the system. For instance, a failed drive will be replaced; multiple drive failure will require all drives be replaced as well the power supply and possibly drive cables if damage is evident. If a system operates for an extended period without cooling fans the system components will be retired from production use and completely replaced.

AUDIT FUNCTIONALITY

Our site monitor audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database, which is kept for a period of time for reporting purposes and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosures. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

There are also numerous reports for data import to track user, date/time, import type, number of records, validity, and total import time.

Audit Reports Available

- Audit Report
- Validity Audit Report
- Field Audit Report
- Run Report
- Run Variance Report

When run incidents enter the system, they are tracked on both date and time and the user that entered that run. It will also track the date/time that a user that last updated that information. In addition to the audit trail, there are addendum and attachment features within the system. Addendums allow staff to enter additional text to track changes within an existing run report, or attach any necessary files.

A history trail for each run report tracks staff usage including date/time and user for:

- Generating PDF Run Reports
- Adding addendums
- Changing run status
- Changing run lock status
- Adding attachments
- Viewing repeat patient

SYSTEM BACKUPS

ImageTrend provide backup coverage for continuity purposes as well as data archive purposes. Define backup and retention policies to clearly establish expectations of coverage. Define continuity resources and locations. Meet or exceed contract and other obligations.

Code Backups

Application code is backed up daily; at least a daily backup exists for all applications hosted in ImageTrend's production environment and is included in hosting costs. These backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. Daily backups are retained for longer as unallocated storage permits but not guaranteed to be available beyond the previous calendar day. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Database Backups

Database files are backed up daily; at least a daily backup exists for any database hosted in ImageTrend's production environment and is included in hosting costs. Daily backups are retained for several days as unallocated storage permits but not guaranteed to be available beyond three previous calendar days. Database backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Restore Procedures

Daily backup files are stored uncompressed to facilitate quick recovery of one or more files as needed. Archive copies are compressed to conserve disk space. All database files are compressed to conserve disk space and must be uncompressed and reattached for restoration. When restoring a file the newer file, if it exists, is renamed and kept before replacing with the backup version. When restoring an entire database file, the copy being replaced is itself backed up before being modified. When restoring part of a database file, the current file is first backed up and the backup database is mounted with a different name, then the needed tables are restored and the backup file is detached. If restoring a complete backup of application code over a corrupted install, a copy of the bad files is kept to maintain any new user-added files since the backup was created.

Backup Goals

ImageTrend has several goals for our backup coverage:

- Provide simple and rapid continuity resources
- Provide adequate backup coverage to meet contract and other obligations
- Substitute redundant active resources for continuity backups where reasonable
- Clearly define specific backup policies which differ from the standards
- Maintain a backup window with minimal impact on performance and availability

Minimal Backup Contents

Backups for all data must include:

- One copy of current application files, updated nightly and stored on separate disks from those hosting the application

- One copy of current database files, updated nightly and stored on separate disks from those hosting the database
- One copy of current system configurations, updated nightly and stored on separate disks from those hosting the system
- Alternate retention policies for a specific application must be laid out in writing, specifying requirements for frequency of backups, retention period and coverage requirements

Archive Backup by category

Standard

- No archive required (0)
- Week of daily archives recommended (8)
- Archives- Minimum: 0, Recommended: 8

Important

- Two weeks of daily archives required (15)
- One month of weekly archives required (4)
- Six months of monthly archives required (6)
- Two months of weekly and 1 year of monthly archives recommended (8,12)
- Archives- Minimum: 25, Recommended: 34

Critical

- Four weeks of daily archives required (29)
- Three months of weekly archives required (12)
- 1 year of monthly archives required (12)
- 1 year of weekly archives recommended (52)
- Archives- Minimum: 53, Recommended: 76

Optional

- No continuity or archives required
- Single continuity backup recommended
- Archives- Minimum: 0, Recommended: 1

Continuity Backup by category

Standard

- Continuity restoration within hours

Important

- Continuity restoration within one hour

Critical

- Continuity restoration within 30 minutes

Optional

- No continuity or archives required

Offsite backup by category

All offsite backups are stored encrypted on disk in a locked fire cabinet in ImageTrend's offices or replicated to other collocation sites per the following categories.

Standard

- Monthly offsite backup is stored

Important

- Monthly offsite backup is stored, offsite replication may be performed per availability requirements

Critical

- Monthly offsite backup is stored, offsite replication may be performed per availability requirements

Optional

- Optical disc based or electronic transmission backups sent to clients may be performed on a negotiated schedule

Terms

Continuity Backup

Data Archive Backup

Full Backup

Incremental Backup

Differential Backup

Week of daily archives

Weekly archive

Monthly archive

Definitions

An exact and current as possible copy of all files, data and system configurations comprising an application

Stored backups for the purposes of restoring data to a specific point in the past

A complete copy of all data at that moment in time

A copy of all new or modified files since last full or incremental backup

A copy of all new or modified files since last full backup

previous week's full backup, this week's full backup and the past six day's nightly differential backups

Full backup made on single day of the week (e.g., Sunday morning)

Full backup made on single day of the month (i.e. the First of the month, or first Sunday of the month)

DISASTER RECOVERY

ImageTrend, Inc. follows a specific critical path for organizations and companies during a recovery effort, to ensure the resumption of normal operations in the event of a disaster. This process has seven stages, which are followed regardless of the organization.

ImageTrend' EMS solutions consist of EMS State Bridge and Field Bridge, hosted at our facilities. In a disaster recovery plan it is important to minimize the loss of data and return application usage as quickly as possible.

Stage 1 - Immediate Response

The first step in the recovery process and the initial reaction to a potential disaster or interruption consists of immediate assessment and if necessary, notification of clients of interruption and any actions they should undertake. In many situations the system's redundancies will accommodate the situation and provide continuity. This takes place within the first 4 hours.

Stage 2 - Environment Restoration

The necessary steps for restoring service via repairs or alternate infrastructure are begun by gathering the necessary components for restoration and installing. If local repair is not possible due to extreme conditions, then the service will be redirected to another data center and the required DNS redirection may take up to 8 hours to propagate.

Stage 3 - Functional Restoration

Application functionality is tested on restored or alternate service site to ensure user access and usability. For same data center restoration within 8 hours and for alternate site usage within 24 hours.

Stage 4 - Data Restoration and Synchronization

This step includes backlog reduction. Data from offsite locations is restored to the restored environment. Database backups are automatically done every 2 hours, daily and weekly. These backups will be used for data restoration and synchronization. Maximum data window will be two hours. Most often, data is protected at different times during the business cycle and must be reconstructed or synchronized before it can be used. Synchronizing, validating, and reviewing data from many different sources is a critical step in a successful recovery. Once reliable data is established, backlogged transactions that have accumulated during recovery can be processed. This may take up to 48 hours, however application usage is available during this time.

Stage 5 - Business Resumption

Clients will be notified that the affected service can now resume its normal operations.

Stage 6 - Interim Site Migration

Once the primary site environment has been restored, return migration is planned and scheduled. Depending on the nature of the problem, this may take an extended period of time to restore the environment. Disruption of services during this transition will be minimized and clients will be notified of the impact and a schedule of return will be mutually discussed.

Stage 7 - Return to Home Site

All recovery efforts have been completed, and a business may resume normal operations at its primary location.

TESTING PROCESSES

SOFTWARE SECURITY VULNERABILITY TESTING

ImageTrend understands the importance of data security and consistently addresses the latest advances in regulations and technologies to ensure that our systems and processes meet federal and state data security standards. Our application security is designed to OWASP best practices and our hosting infrastructure is the latest 3-tier firewall configuration. Application access utilizes 128 bit encrypted secure socket layers and data transfers are encrypted as well. Our QA includes the use of IBM AppScan, which provides:

- Static analysis security testing to identify vulnerabilities at the source
- Automated web application scanning and testing with intelligent fix recommendations
- Extended coverage through Glassbox analysis and JavaScript Security Analyzer
- Automated correlation of static and dynamic analysis results

Security reviews have been conducted by several individual government organizations prior to their purchase of our applications with satisfactory results.

ADA TESTING PROCESS

ImageTrend follows ADA WCAG 2.0 level conformance guidelines. Resources are created and designed using xml, css, mathml, SMIL, SVG and other open standards that have features to support accessibility by people with disabilities. The client-facing pages follow the standards set in the ADA WCAG 2.0 accessibility guidelines to level AA conformance. ImageTrend performs audits of its product's accessibility and works to improve its conformance through regularly scheduled product upgrades. As with all of its products, ImageTrend, Inc. extends an ongoing effort to conform application to Level AA – ADA Conformance for Web Content Guidelines. We offer all of our clients the opportunity to perform testing on our web based applications to determine compliance with their own policies, needs, and/or requests. Should these tests result in modification or enhancement requests, they will be reviewed as to applicability within our planned product roadmap or handled as client-specific requests.

INFORMATION SENSITIVITY POLICY

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of ImageTrend without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing).

All employees familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect ImageTrend Confidential information (e.g., ImageTrend Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager.

Data Privacy

ImageTrend respects and understands the need for data privacy and the methods and functions needed to ensure this for both ImageTrend data and Client data. Software application, data center infrastructure, policies and procedures all play an integral role in this. Our staff reviews all updates whether from our partners (Microsoft and Adobe), federal and state legal opinions and guidelines or standards organizations to ensure that we are continually informed of the latest requirements. Our designers and developers continually monitor best practices and technological advances to ensure data privacy. ImageTrend's data center is located in a bank vault and has all of the physical controls in place to ensure security. Our staff is trained in the needs and processes required for data privacy and are all subjected to background checks.

On an annual basis, unless previous action was required, we review our security policies and procedures to ensure that necessary updates have occurred. We welcome any security reviews that our customers might request at their expense. Several clients have performed such reviews over the years and have been satisfied with the results.

HIPAA Training

All ImageTrend employees are subjected to background checks and are required to attend and successfully complete HIPAA training. The ImageTrend Project Management System gives us a facility to track any HIPAA Security Incidents or Information Disclosure Incidents for reporting purposes.

Only those certified ImageTrend employees that work with either hardware or software related to the specified application or project will access the data center and interact with our servers. These employees have worked with our hardware as part of our IT support staff or are part of our Implementation team as software developers. Authorization is granted from the management level.

Scope

All ImageTrend information is categorized into two main classifications:

- ImageTrend Public
- ImageTrend Confidential

ImageTrend Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to ImageTrend Systems, Inc.

ImageTrend Confidential contains all other information. Confidential information is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Information that should be protected very closely includes trade secrets, development programs, potential acquisition targets and other information integral to the success of our company. Also included in ImageTrend Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of ImageTrend Confidential information is "ImageTrend Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to ImageTrend by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders and supplier information. Information in this category ranges from extremely sensitive to information about connecting a supplier/vendor into ImageTrend's network to support our operations.

ImageTrend personnel are encouraged to use common sense judgment in securing ImageTrend Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their manager.

Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as ImageTrend Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the ImageTrend Confidential information in question.

Minimal Sensitivity

Minimal sensitivity data includes general corporate information and some personnel and technical information.

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential."

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "ImageTrend Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "ImageTrend Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, ImageTrend information is presumed to be "ImageTrend Confidential" unless expressly determined to be ImageTrend Public information by an ImageTrend employee with authority to do so.

Guidelines for Minimal Security Data

- **Access.** Granted to ImageTrend employees, contractors, people with a business need to know.
- **Distribution within ImageTrend.** Allowed in standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Allowed with U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

- **Electronic distribution.** No restrictions except that it is sent to only approved recipients.
- **Storage.** Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- **Disposal/Destruction.** Deposit outdated paper information in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive

More sensitive data includes business, financial, technical and most personnel information

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential."

As the sensitivity level of the information increases, in addition to or instead of marking the information "ImageTrend Confidential" or "ImageTrend Proprietary," you may wish to label the information "ImageTrend Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Guidelines for More Sensitive Data

- **Access.** Granted to ImageTrend employees and non-employees with signed non-disclosure agreements who have a business need to know.
- **Distribution within ImageTrend.** Allowed with standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Can be sent via U.S. mail or approved private carriers.
- **Electronic distribution.** No restrictions on sending to approved recipients within ImageTrend, but should be encrypted or sent via a private link to approved recipients outside of ImageTrend premises.
- **Storage.** Individual access controls are highly recommended for electronic information.
- **Disposal/Destruction.** Allowed in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code and technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

To indicate that ImageTrend Confidential information is very sensitive, you may should label the information "ImageTrend Internal: Registered and Restricted", "ImageTrend Eyes Only," "ImageTrend Confidential" or similar labels at the discretion of your individual

business unit or department. Once again, this type of ImageTrend Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Guidelines for Most Sensitive Data

- **Access.** Granted to only those individuals (ImageTrend employees and non-employees) designated with approved access and signed non-disclosure agreements.
- **Distribution within ImageTrend.** Must be delivered direct — signature required, envelopes stamped confidential or approved electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Must be delivered direct; signature required; approved private carriers.
- **Electronic distribution.** No restriction to approved recipients within ImageTrend, but it is highly recommended that all information be strongly encrypted.
- **Storage.** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
- **Disposal/Destruction.** This is strongly encouraged: Should be in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Terms

Appropriate measures

Definitions

To minimize risk to ImageTrend from an outside business connection, ImageTrend computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access ImageTrend corporate information, the amount of information at risk is minimized.

Configuration of ImageTrend-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot; instead, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within ImageTrend is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information

and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac, you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of ImageTrend.

Encryption

Secure ImageTrend Sensitive Information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a onetime password token to connect to ImageTrend's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that ImageTrend has control over for its entire distance. For example, all ImageTrend networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. ISDN lines to employees' homes are private links. ImageTrend also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies with which ImageTrend has established private links include all announced acquisitions and some short-term temporary links

PHYSICAL SECURITY OF OFFICE AND HOSTING SITE

Entrances

Facility and office entrances are kept to a minimum to control access. ImageTrend's main entrance is planned with access control systems and procedures in mind. Reception desk and other controls help to maintain security at ImageTrend's front entrance. The other entrances at the ImageTrend office are only accessible by employees with keys.

Access Controls

At every perimeter entrance, locking devices and controls are in place to ensure security is sustained. Key control is an essential part to ImageTrend's access control. Only ImageTrend employees are given a key that cannot be replicated. Before 8:00 am and after 5:00pm all ImageTrend entrances are locked. To get in or out before 8:00 am or after 5:00pm employees need to unlock the door to enter, and then relock the entrance behind them.

Exterior Security

ImageTrend equips the building with security cameras that run 24/7. These security cameras monitor activities outside the building to provide views of approaching pedestrian and vehicular traffic, building entrances, and departing pedestrian and vehicular traffic.

Physical Security of Hosting Site

All visitors of Implex.net are greeted and asked to sign in with photo ID. The visitors are escorted around the facility by an Implex.net employee. The Implex.net site has video surveillance and two controlled doors with key card access.

All visitor information, not just the sensitive information, is restricted to Implex.net developers, network operations personnel and other qualified employees (such as billing clerks or customer care representatives). Finally, the servers on which Implex.net stores personally identifiable information are kept in a secure location.

The DataSafe is Implex.net's main data center where they collocate servers and host client web sites on their shared servers. The entry to the Implex.net DataSafe was built inside a bank vault and is thoroughly encased by 21" reinforced concrete walls. The vault doors are fully functional.

REMOTE ACCESS POLICY

The purpose of this policy is to define standards for connecting to ImageTrend's network from any host. These standards are designed to minimize the potential exposure of ImageTrend to damages that may result from unauthorized use of ImageTrend resources. Damages include the loss of sensitive or company confidential data, loss of intellectual property, damage to public image, damage to critical ImageTrend internal systems, etc.

Scope

This policy applies to all ImageTrend employees, contractors, vendors and agents with an ImageTrend-owned or personally-owned computer or workstation used to connect to the ImageTrend network. This policy applies to remote access connections used to do work on behalf of ImageTrend, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH and cable modems, etc.

Policy

General

It is the responsibility of ImageTrend employees, contractors, vendors and agents with remote access privileges to ImageTrend's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ImageTrend.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods and of acceptable use of ImageTrend's network:

- Acceptable Encryption Policy
- Virtual Private Network (VPN) Policy
- Wireless Communications Policy
- Acceptable Use Policy

For additional information regarding ImageTrend's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases whenever possible. Use of a username/password combination is acceptable for access when DACL's are applied. For information on creating a strong passphrase see the Password Policy.

- At no time should any ImageTrend employee provide their login or email password to anyone, not even family members.
- ImageTrend employees and contractors with remote access privileges must ensure that their ImageTrend-owned or personal computer or workstation, which is remotely connected to ImageTrend's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- ImageTrend employees and contractors with remote access privileges to ImageTrend's corporate network must not use non-ImageTrend email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct ImageTrend business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the ImageTrend network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
- All hosts that are connected to ImageTrend internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
- Personal equipment that is used to connect to ImageTrend's networks must meet the requirements of ImageTrend-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the ImageTrend production network must obtain prior approval from Remote Access Services and InfoSec.

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol (CHAP) is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: being logged into the Corporate network via a local Ethernet connection and dialing into AOL or other Internet service provider (ISP); being on an ImageTrend-provided Remote Access home network and connecting to another network (such as a spouse's remote access); or configuring an ISDN router to dial into ImageTrend and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is another form of high-speed Internet access. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that can go incrementally from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network (ISDN): BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to ImageTrend's corporate network through a non-ImageTrend controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-ImageTrend network (such as the Internet or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into ImageTrend's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

ROLES AND RESPONSIBILITIES

Roles of system administrators in terms of their responsibility for defining and securing access for users are as follows:

Role	Responsibilities
Administrators (X-Team)	Full access to infrastructure, operating systems and supporting applications
Implementation	Full control of code, database tables and supporting applications
Level 1 Support	User level access to the ImageTrend application
Level 2 Support	Admin level access to the ImageTrend application and limited access to the supporting applications
Level 3 Support	SuperAdmin rights to the ImageTrend application read rights to the database and can change accounts and permissions

INCIDENT REPORT MECHANISM

Effective response and collective action are required to counteract security violations and activities that lead to security breaches. ImageTrend shall provide timely and appropriate notice to affected clients when there is reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information, typically maintained in an electronic format by ImageTrend.

Purpose

The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations. It is important to distinguish between problems that stem from mistakes or miscommunications and true security incidents that involve either malicious intent or intent to circumvent security measures

Scope

Attacks on ImageTrend resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on ImageTrend systems and/or on ImageTrend networks to appropriate authorities is a requirement of all persons affiliated with ImageTrend in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

General

Suspected or confirmed information security breaches must be reported to ImageTrend. ImageTrend will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform the IT Manager and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the IT Manager will consult with the appropriate ImageTrend employees to develop the response and make the final determination if a public notification of the event is warranted.

Procedures

The entity responsible for support of the system or network under attack is expected to:

- Report the attack to their management and to the IT Manager
- Block or prevent escalation of the attack, if possible
- Follow instructions communicated from the IT Manager in subsequent investigation of the incident and preservation of evidence
- Implement recommendations from the IT Manager
- Repair the resultant damage to the system

Internal Notifications

ImageTrend's employees will report serious computer security breaches to the IT Manager in a timely manner. The IT Manager will consult with one or more VP's as appropriate, and decides if the Management Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach.

External Notification

Determination of External Notification

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

- Physical possession (lost or stolen device?)
- Credible evidence the information was copied/removed
- Length of time between intrusion and detection

- Purpose of the intrusion was acquisition of information
- Credible evidence the information was in a useable format
- Ability to reach the affected individuals
- Applicable University policy, and/or local, state, or federal laws

External Notification

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

- Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists. The letter will be developed by the department responsible for the system experiencing the breach, and approved by the Management Team and others as appropriate. The excessiveness of cost consideration will be the decision of the IT Manager, Management Team, and President for.

If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

- Personal e-mail notices (provided addresses are available), developed by the department responsible for the system experiencing the breach, and approved by the IT Manager, Management Team, and other administrators as appropriate.
- A press release to media, to be written by Marketing and approved by the IT Manager, and other administrators as appropriate.
- An informational web site, developed and hosted by the department responsible for the system experiencing the breach, and approved by the IT Manager, Management Team, and others as appropriate, with a conspicuous link in the ImageTrend News area.
- All expenses associated with external notification will be the responsibility of the department responsible for the system that experienced the security breach.

SUPPORT SERVICES

ImageTrend provides both support for their applications and hosting as contracted. Support includes technical diagnosis and fixes of technology issues involving software and server hardware. ImageTrend has a broad range of technical support and proposes to provide service in the areas of:

- Website Hosting and Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

Product Support

ImageTrend will provide ongoing support as contracted after installation for the customer. This includes continued attention to product performance and general maintenance. ImageTrend offers multi-level technical support, based on level-two user support by accommodating both the general inquiries of the administrators and those of the system users. We will give the administrators the ability to field support for the system as the first level of contact while providing them the option to refer inquiries directly to ImageTrend.

ImageTrend's Support Team is available 24/7 at support@imagetrend.com and www.imagetrend.com/support as well as Monday through Friday from 7:00 am to 7:00 pm CST at:

Toll Free: 1-888-469-7789

Phone: 952-469-1589

Support Desk

ImageTrend offers an online support system, Support Desk, which incorporates around-the-clock incident reporting of all submitted tickets to ImageTrend's support desk specialists. Once a client submits a support ticket, he or she can easily track its progress with a secure login, promoting a support log for the client and

ImageTrend's support team. The system promotes speedy resolution by offering keyword-based self-help services and articles in the knowledgebase, should clients wish to bypass traditional support services. Ticket tracking further enhances the efforts of Support Desk personnel by allowing them to identify patterns which can then be utilized for improvements in production, documentation, education and frequently asked questions to populate the knowledgebase. The support ticket tracking system ensures efficient workflow for the support desk specialists while keeping users informed of their incident's status. Support patterns can be referenced to populate additional knowledgebase articles.

Upgrades and New Version Releases

ImageTrend offers updates and new version releases to customers subscribing to our support agreements. On average, these updates occur once a quarter. These updates offer new product enhancements and improvements. Customers are notified in advance of these potential changes in order for them to be aware of any impact this may have on them and to schedule the upgrade. The Fire Bridge, if hosted at our facilities, is upgraded by our personnel; however clients are notified prior to the upgrade for scheduling purposes. If the Fire Bridge is hosted at your facilities, then we assist in the upgrade either through remote login or an onsite visit if required (incurs travel costs).

The contents of the updates are determined by customer request levels and necessity. The EDS Users Group, comprised of field EMT's and Paramedics, has also been instrumental in providing insight for determining the necessity and value of requested product enhancements.

ImageTrend support agreements include software updates, so that applications continually offer the latest technology and provide new features. We encourage all clients to take advantage of these updates. Products will be maintained for the client as long as they have a valid support agreement.

X-Team Support

In addition to our standard services, ImageTrend's X-Team is available for after-hour's emergency support. Our X-Team will receive notifications of issues submitted to our Online Support Desk. If an issue is deemed non-critical by the X-team they may elect to respond during normal business hours or charge for after hour's resolution.

Problem Escalation and Resolution

ImageTrend has support available for clients via telephone, Support Desk and/or electronic mail during ImageTrend's normal business hours (7:00 a.m. to 7:00 p.m. Central Standard Time, Monday through Friday, excluding holidays). The Project Manager will address operational issues on an ongoing basis. Senior Management will handle issues requiring further discussion and resolution.

Incident Reporting

Malfunctions. ImageTrend makes all efforts to correct malfunctions that are documented and reported by the Client. ImageTrend acknowledges receipt of a malfunction report from a Client and acknowledges the disposition and possible resolution thereof according to the Service Level Agreement. If the Malfunction reported prevents all useful work from being done, or disables major functions from being performed, we undertake immediate corrective action to remedy the reported issue. If the malfunction reported represents a non-mission critical issue, reasonable corrective action to remedy the malfunction within three business days will be taken. If the malfunction reported disables only non-essential functions, resulting in degraded operations, we undertake reasonable corrective action to remedy the reported malfunction within a reasonable time period.

Submission. All support requests received by either direct phone contacts, Support Desk and support@imagetrend.com are recorded by client, incident description and disposition into our support log.

Support Log

Information regarding outstanding problems, fixes, modifications and improvements will be available to the Client electronically and published on a regular basis to a Project Support Log which will be available for Client's access.

ImageTrend University

ImageTrend provides online education materials for their products as self-guided tutorials to all clients with support agreements. These online support and educational materials can be found at ImageTrend

University via your ImageTrend application. ImageTrend recently started implementing ImageTrend University throughout its solutions to promote ongoing education and training of our solutions. When accessing ImageTrend University through the application, users can view educational videos, manuals, quick guides and workbooks to assist them in better understanding our software and support train-the-trainer sessions. These have been very useful as both refresher and initial education materials. A sample demonstration of ImageTrend University can be found at www.imagetrend.com/university.

System Documentation

ImageTrend provides the most up-to-date documentation, including administrator and user manuals and release notes for any upgrades. With a support agreement, this documentation, along with educational videos, PowerPoint presentations and other documents will be found at ImageTrend University, which can be accessed from the State Bridge application. Any provided documentation becomes the property of the client. ImageTrend will provide a full set of documentation at each location upon request. Documentation updates are available online at no cost.

System Maintenance

Change Request. When a client makes a change request, we apply that to other users and their needs to determine if it would be beneficial to others in the EMS community – from the local volunteer organization to the regional users to mid and large size cities and state governments. If the requested change would be beneficial to the product as a whole, it may be included in a version release. For client-specific requests, we seek further mutual understanding. Sometimes product understanding meets the intended outcome of the change request or a work around is found. If neither of these meets the needs of the client, we can establish a Statement of Work to customize the application for the specific client for additional fees.

Support Staff. ImageTrend's support staff is made up of EMS and Fire professionals who are well versed in the technical aspects of our products. They are either well trained on the software, have used it in the field, or are the developers of the system.



Table 3: Future Initiatives – Rate Card

Resource Type	Not-to-Exceed Hourly Rate (\$)
Project management	\$125.00
Business analysts	\$125.00
System analysts	\$125.00
Programmer/developers	\$125.00
System administrators	\$125.00
Database administrators	\$125.00
Q/A Manager	\$125.00
Security specialist	\$125.00
Testers	\$125.00
Technical writers	\$125.00
CM specialists	\$125.00
System Architects	\$125.00
Network engineer/administrator	\$125.00
Software Architects	\$125.00
CM specialists	\$125.00
Project assistants	\$125.00
Web developers	\$125.00
Application trainers	\$125.00
Others: (List) below:	

Notes:

The State may request additional Position Types, other than the Position Types listed above during the contract term.



ImageTrend Price Breakdown

Hosting and Maintenance	Description	Qty	Price	Extended Price
	EMS State Bridge Annual Support 4/01/2014-9/30/2014	1	\$14,720.00	\$14,720.00
	EMS State Bridge Annual Hosting 4/01/2014-9/30/2014	1	\$10,200.00	\$10,200.00
	Visual Informatics (Data Mining) Annual Support 4/01/2014-9/30/2014	1	\$4,800.00	\$4,800.00
	Patient Registry (Trauma Bridge) Annual Support 4/01/2014-9/30/2014	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Hosting 4/01/2014-9/30/2014	1	\$3,600.00	\$3,600.00
	Total for Year Ending September 30, 2014:			\$42,920.00
	EMS State Bridge Annual Support 10/01/2014-9/30/2015	1	\$29,440.00	\$29,440.00
	EMS State Bridge Annual Hosting 10/01/2014-9/30/2015	1	\$20,400.00	\$20,400.00
	Visual Informatics (Data Mining) Annual Support 10/01/2014-9/30/2015	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Support 10/01/2014-9/30/2015	1	\$19,200.00	\$19,200.00
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2014-9/30/2015	1	\$7,200.00	\$7,200.00
	Total for Year Ending September 30, 2015:			\$85,840.00
	EMS State Bridge Annual Support 10/01/2015-9/30/2016	1	\$29,440.00	\$29,440.00
EMS State Bridge Annual Hosting 10/01/2015-9/30/2016	1	\$20,400.00	\$20,400.00	
Visual Informatics (Data Mining) Annual Support 10/01/2015-9/30/2016	1	\$9,600.00	\$9,600.00	
Patient Registry (Trauma Bridge) Annual Support 10/01/2015-9/30/2016	1	\$19,200.00	\$19,200.00	
Patient Registry (Trauma Bridge) Annual Hosting 10/01/2015-9/30/2016	1	\$7,200.00	\$7,200.00	
Total for Year Ending September 30, 2016:			\$85,840.00	
EMS State Bridge Annual Support 10/01/2016-9/30/2017	1	\$29,440.00	\$29,440.00	
EMS State Bridge Annual Hosting 10/01/2016-9/30/2017	1	\$20,400.00	\$20,400.00	
Visual Informatics (Data Mining) Annual Support 10/01/2016-9/30/2017	1	\$9,600.00	\$9,600.00	
Patient Registry (Trauma Bridge) Annual Support 10/01/2016-	1	\$19,200.00	\$19,200.00	



	9/30/2017			
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2016-9/30/2017	1	\$7,200.00	\$7,200.00
	Total for Year Ending September 30, 2017:			\$85,840.00
	EMS State Bridge Annual Support 10/01/2017-9/30/2018	1	\$29,440.00	\$29,440.00
	EMS State Bridge Annual Hosting 10/01/2017-9/30/2018	1	\$20,400.00	\$20,400.00
	Visual Informatics (Data Mining) Annual Support 10/01/2017-9/30/2018	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Support 10/01/2017-9/30/2018	1	\$19,200.00	\$19,200.00
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2017-9/30/2018	1	\$7,200.00	\$7,200.00
	Total for Year Ending September 30, 2018:			\$85,840.00
	EMS State Bridge Annual Support 10/01/2018-9/30/2019	1	\$29,440.00	\$29,440.00
	EMS State Bridge Annual Hosting 10/01/2018-9/30/2019	1	\$20,400.00	\$20,400.00
	Visual Informatics (Data Mining) Annual Support 10/01/2018-9/30/2019	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Support 10/01/2018-9/30/2019	1	\$19,200.00	\$19,200.00
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2018-9/30/2019	1	\$7,200.00	\$7,200.00
	Total for Year Ending September 30, 2019:			\$85,840.00
	Ongoing Annual Fees for Optional Years*:			\$85,840.00
	<i>*May be subject to Consumer Price Index increases as defined in the contract.</i>			
OPTIONAL	Custom Development Allowance - Requires Statement of Work. May incur additional Hosting and/or Support Fees. Up to 1500 hours billed as used.	1	\$187,500.00	
	Upgrade to State Rescue Bridge	1	\$120,000.00	
	Upgrade to State Rescue Bridge Annual Support	1	\$19,200.00	
	Upgrade to State Rescue Bridge Annual Hosting	1	\$9,000.00	
	Upgrade to State Rescue Bridge Project Management and Setup	1	\$10,000.00	
	Field Bridge Statewide Site License	1	\$120,000.00	
	Field Bridge Statewide Site License Annual Support	1	\$19,200.00	
	MARS (Mapping and Reporting System) Setup	1	\$15,000.00	
	MARS Annual Transactional Fee	1	\$12,000.00	



Hospital Dashboard Setup	1	\$24,000.00	
Hospital Dashboard Annual Support	1	\$3,840.00	
Visual Informatics (Data Mining) Cubes:			
Fire Cube	1	\$6,000.00	
Fire Cube Annual Support	1	\$960.00	
Trauma (Incident) Cube	1	\$6,000.00	
Trauma Cube Annual Support	1	\$960.00	
Resource Bridge Cube	1	\$6,000.00	
Resource Bridge Annual Support	1	\$960.00	
Patient Registry Categories (Forms):			
Trauma Follow-up Category	1	\$18,000.00	
Trauma Follow-up Annual Support	1	\$2,880.00	
Trauma Follow-up Annual Hosting	1	\$1,200.00	
STEMI Category	1	\$25,000.00	
STEMI Category Annual Support	1	\$4,000.00	
STEMI Category Annual Hosting	1	\$1,500.00	
Stroke Category	1	\$25,000.00	
Stroke Category Annual Support	1	\$4,000.00	
Stroke Category Annual Hosting	1	\$1,500.00	
Burn Category	1	\$25,000.00	
Burn Category Annual Support	1	\$4,000.00	
Burn Category Annual Hosting	1	\$1,500.00	
Submersion Category	1	\$25,000.00	
Submersion Category Annual Support	1	\$4,000.00	
Submersion Category Annual Hosting	1	\$1,500.00	
Rehabilitation Category	1	\$25,000.00	
Rehabilitation Category Annual Support	1	\$4,000.00	
Rehabilitation Category Annual Hosting	1	\$1,500.00	
License Management License Fee	1	\$80,000.00	
License Management Annual Support	1	\$21,600.00	
License Management Annual Hosting	1	\$9,000.00	
License Management Project Management and Setup	1	\$10,000.00	



Personnel Licensure for First Responder, EMT-B, EMT-Advanced / Intermediate, EMT-P Types	1	\$20,000.00	
Vehicles Licensure for Ambulances	1	\$5,000.00	
Services/Agency Licensure for Ground, Air and Private	1	\$20,000.00	
Payment Gateway (TBD)	1	\$10,000.00	
Resource Bridge Base Platform	1	\$50,000.00	
Resource Bridge Base Platform Annual Support	1	\$8,000.00	
Resource Bridge Base Platform Annual Hosting (99.99%)	1	\$24,000.00	
Resource Bridge Base Platform Project Management & Setup	1	\$10,000.00	
Resource Bridge Additional Modules (requires purchase of Resource Bridge Base Platform):			
Alert Manager Setup	1	\$15,000.00	
Alert Manager Annual Support	1	\$2,400.00	
Alert Manager Annual Hosting	1	\$3,000.00	
Inventory Setup	1	\$25,000.00	
Inventory Annual Support	1	\$4,000.00	
Inventory Annual Hosting	1	\$3,600.00	
Procurement Setup	1	\$50,000.00	
Procurement Annual Support	1	\$8,000.00	
Procurement Annual Hosting	1	\$4,800.00	
Bed Tracking (includes HavBED export) with Specialties Setup	1	\$30,000.00	
Bed Tracking Annual Support	1	\$4,800.00	
Bed Tracking Annual Hosting	1	\$4,800.00	
Diversion Status (with Regional Status) Setup	1	\$15,000.00	
Diversion Status Annual Support	1	\$2,400.00	
Diversion Status Annual Hosting	1	\$3,000.00	
Fatality Tracking Web Module Setup	1	\$50,000.00	
Fatality Tracking Web Module Annual Support	1	\$8,000.00	
Fatality Tracking Web Module Annual Hosting	1	\$4,800.00	
Fatality Tracking Mobile Setup	1	\$25,000.00	
Fatality Tracking Mobile Annual Support	1	\$4,000.00	
Fatality Tracking Mobile Annual Hosting	1	\$3,600.00	



MAPS API Setup	1	\$10,000.00	
MAPS API Annual Support	1	\$1,600.00	
MAPS API Annual Hosting	1	\$2,400.00	
Resource Request Setup	1	\$15,000.00	
Resource Request Annual Support	1	\$2,400.00	
Resource Request Annual Hosting	1	\$3,000.00	
Command Center Setup	1	\$30,000.00	
Command Center Annual Support	1	\$4,800.00	
Command Center Annual Hosting	1	\$4,800.00	
Command Post Setup	1	\$15,000.00	
Command Post Annual Support	1	\$2,400.00	
Command Post Annual Hosting	1	\$3,000.00	
Patient Tracking Web Module Setup	1	\$30,000.00	
Patient Tracking Web Annual Support	1	\$4,800.00	
Patient Tracking Web Annual Hosting	1	\$4,800.00	
Patient Tracking Mobile Setup	1	\$25,000.00	
Patient Tracking Mobile Annual Support	1	\$4,000.00	
Patient Tracking Mobile Annual Hosting	1	\$3,600.00	
Document Hub Setup	1	\$10,000.00	
Document Hub Annual Support	1	\$1,600.00	
Hospital Hub Setup	1	\$30,000.00	
Hospital Hub Annual Support	1	\$4,800.00	
Hospital Hub Annual Hosting	1	\$4,800.00	
Onsite Training Sessions @ \$1,500 per day per trainer	1	\$1,500.00	
Custom Development - Out of Scope billed at \$125.00 per hour - requires separate Statement of Work	TBD	\$125.00	

Notes:

- a. ImageTrend agrees to offer a 10% discount on all one-time fees. This discount is valid for 90 days after contract signature. This would allow the State to select any optional items that they would like to move forward with in the near future at the discounted rate.
- b. ImageTrend agrees to lock-in the discounted rate on the one-time fees for the STEMI, Stroke and Burn Categories of the Patient Registry System provided they are included in the contract and will pro-rate any Annual Fees based on the implementation date of these items to align with the State's fiscal Year (10/1-9/30).



The initial value of spending authority for future initiatives to the Contract is \$249,000.00. Actual funding for future initiatives will occur on a yearly basis, and there is no guarantee as to the level of funding, if any, available to the project. The State makes no guarantee that any additional license(s), optional software/modules or technical services will be procured. The state reserves the right to purchase additional license(s), optional software/modules or technical services through other State contracts.

The State shall have the right to hold back an amount equal to percent 10% of all amounts invoiced by Contractor for specified deliverables for future enhancements. The amounts held back shall be released to Contractor after the State has granted Final Acceptance.

Future enhancements must be dependent upon mutually agreed upon statement(s) of work (SOW) between the Contractor and the State of Michigan. Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a statement of work until authorized via a purchase order issued against this contract.

Each SOW will include:

1. Background
2. Project Objective
3. Scope of Work
4. Deliverables
5. Acceptance Criteria
6. Project Control and Reports
7. Specific Department Standards
8. Cost/Rate
9. Payment Schedule
10. Project Contacts
11. Agency Responsibilities
12. Location of Where the Work is to be performed
13. Expected Contractor Work Hours and Conditions

The parties agree that the Services/Deliverables to be rendered by Contractor pursuant to this Contract (and any future amendments of it) will be defined and described in detail in a SOW.

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 530 W. ALLEGAN, LANSING, MI 48933

**NOTICE
 OF
 CONTRACT NO. 071B4300073**
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Imagetrend, Inc. 20855 Kensington Blvd Lakeville, MN 55044	Trisha Moline	tmoline@imagetrend.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(952) 469-1589	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:	TBD	TBD	TBD	TBD
BUYER:	DTMB	Whitnie Zuker	517-284-7030	Zukerw@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Descriptive Contract Title (Not always the same language as provided in MAIN)			
Michigan Emergency Medical Services Information System (MEMSIS)			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
	4/1/2014	9/30/2019	5
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
45			
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MiDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
MISCELLANEOUS INFORMATION:			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:		\$721,120.00	

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation # 0071141114B0001030 (084R4300009). Orders for delivery will be issued directly by the Department of Technology, Management & Budget through the issuance of a Purchase Order Form.

Notice of Contract #: 071B4300073

FOR THE CONTRACTOR:	FOR THE STATE:
_____ Firm Name	_____ Signature
_____ Authorized Agent Signature	_____ Name/Title
_____ Authorized Agent (Print or Type)	_____ Enter Name of Agency
_____ Date	_____ Date

STATE OF MICHIGAN
 DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
 PROCUREMENT
 P.O. BOX 30026, LANSING, MI 48909
 OR
 530 W. ALLEGAN, LANSING, MI 48933

CONTRACT NO. 071B4300073
 between
THE STATE OF MICHIGAN
 and

NAME & ADDRESS OF CONTRACTOR:	PRIMARY CONTACT	EMAIL
Imagetrend, Inc. 20855 Kensington Blvd Lakeville, MN 55044	Trisha Moline	tmoline@imagetrend.com
	TELEPHONE	CONTRACTOR #, MAIL CODE
	(952) 469-1589	

STATE CONTACTS	AGENCY	NAME	PHONE	EMAIL
CONTRACT COMPLIANCE INSPECTOR:	TBD	TBD	TBD	TBD
BUYER:	DTMB	Whitnie Zuker	517-284-7030	Zukerw@michigan.gov

CONTRACT SUMMARY:			
DESCRIPTION: Descriptive Contract Title (Not always the same language as provided in MAIN)			
Michigan Emergency Medical Services Information System (MEMSIS)			
INITIAL TERM	EFFECTIVE DATE	INITIAL EXPIRATION DATE	AVAILABLE OPTIONS
	4/1/2014	9/30/2019	5
PAYMENT TERMS	F.O.B	SHIPPED	SHIPPED FROM
45			
ALTERNATE PAYMENT OPTIONS:			AVAILABLE TO MiDEAL PARTICIPANTS
<input type="checkbox"/> P-card <input type="checkbox"/> Direct Voucher (DV) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
MINIMUM DELIVERY REQUIREMENTS:			
MISCELLANEOUS INFORMATION:			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION:			\$721,120.00

THIS IS NOT AN ORDER: This Contract Agreement is awarded on the basis of our inquiry bearing the solicitation # 0071141114B0001030 (084R4300009). Orders for delivery will be issued directly by the Department of Technology, Management & Budget through the issuance of a Purchase Order Form.

Notice of Contract #: 071B4300073

FOR THE CONTRACTOR:	FOR THE STATE:
_____ Firm Name	_____ Signature
_____ Authorized Agent Signature	_____ Name/Title
_____ Authorized Agent (Print or Type)	_____ Enter Name of Agency
_____ Date	_____ Date

Table of Contents

<u>Article 1 – Statement of Work (SOW)</u>		9
<u>1.000</u>	<u>Project Identification</u>	9
	<u>1.001 Project Request</u>	9
	<u>1.002 Background</u>	9
<u>1.100</u>	<u>Scope of Work and Deliverables</u>	9
	<u>1.101 In Scope</u>	9
	<u>1.102 Out Of Scope</u>	10
	<u>1.103 Environment</u>	10
	<u>1.104 Work And Deliverable</u>	11
<u>1.200</u>	<u>Roles and Responsibilities</u>	18
	<u>1.201 Contractor Staff, Roles, And Responsibilities</u>	18
	<u>1.202 State Staff, Roles, And Responsibilities</u>	19
<u>1.300</u>	<u>Project Plan</u>	20
	<u>1.301 Project Plan Management</u>	20
<u>1.600</u>	<u>Compensation and Payment</u>	24
	<u>1.601 Compensation And Payment</u>	24
<u>Article 2, Terms and Conditions</u>		27
<u>2.000</u>	<u>Contract Structure and Term</u>	27
	<u>2.001 Contract Term</u>	27
	<u>2.002 Options to Renew</u>	27
	<u>2.003 Legal Effect</u>	27
	<u>2.004 Attachments & Exhibits</u>	27
	<u>2.005 Ordering</u>	27
	<u>2.006 Order of Precedence</u>	27
	<u>2.007 Headings</u>	28
	<u>2.008 Form, Function & Utility</u>	28
	<u>2.009 Reformation and Severability</u>	28
<u>2.010</u>	<u>Consents and Approvals</u>	28
	<u>2.011 No Waiver of Default</u>	28
	<u>2.012 Survival</u>	28
<u>2.020</u>	<u>Contract Administration</u>	28
	<u>2.021 Issuing Office</u>	28
	<u>2.022 Contract Compliance Inspector</u>	29
	<u>2.023 Project Manager</u>	29
	<u>2.024 Change Requests</u>	29
	<u>2.025 Notices</u>	30
	<u>2.026 Binding Commitments</u>	31
	<u>2.027 Relationship of the Parties</u>	31
	<u>2.028 Covenant of Good Faith</u>	31
	<u>2.029 Assignments</u>	31
<u>2.030</u>	<u>General Provisions</u>	31
	<u>2.031 Administrative Fee and Reporting</u>	31
	<u>2.032 Media Releases</u>	32
	<u>2.033 Contract Distribution</u>	32
	<u>2.034 Permits</u>	32
	<u>2.035 Website Incorporation</u>	32
	<u>2.036 Future Bidding Preclusion</u>	32
	<u>2.037 Freedom of Information</u>	32
	<u>2.038 Disaster Recovery</u>	32
<u>2.040</u>	<u>Financial Provisions</u>	33
	<u>2.041 Fixed Prices for Services/Deliverables</u>	33
	<u>2.042 Adjustments for Reductions in Scope of Services/Deliverables</u>	33
	<u>2.043 Services/Deliverables Covered</u>	33

2.044	Invoicing and Payment – In General	33
2.045	Pro-ration	34
2.046	Antitrust Assignment	34
2.047	Final Payment	34
2.048	Electronic Payment Requirement	34
2.050	Taxes	34
2.051	Employment Taxes	34
2.052	Sales and Use Taxes	35
2.060	Contract Management	35
2.061	Contractor Personnel Qualifications	35
2.062	Contractor Key Personnel	35
2.063	Re-assignment of Personnel at the State's Request	36
2.064	Contractor Personnel Location	36
2.065	Contractor Identification	36
2.066	Cooperation with Third Parties	36
2.067	Contract Management Responsibilities	36
2.068	Contractor Return of State Equipment/Resources	36
2.070	Subcontracting by Contractor	37
2.071	Contractor full Responsibility	37
2.072	State Consent to delegation	37
2.073	Subcontractor bound to Contract	37
2.074	Flow Down	37
2.075	Competitive Selection	37
2.080	State Responsibilities	38
2.081	Equipment	38
2.082	Facilities	38
2.090	Security	38
2.091	Background Checks	38
2.100	Confidentiality	38
2.101	Confidentiality	38
2.102	Protection and Destruction of Confidential Information	38
2.103	PCI DATA Security Standard	39
2.104	Exclusions	39
2.105	No Implied Rights	39
2.106	Security Breach Notification	40
2.107	Respective Obligations	40
2.110	Records and Inspections	40
2.111	Inspection of Work Performed	40
2.112	Retention of Records	40
2.113	Examination of Records	40
2.114	Audit Resolution	40
2.115	Errors	41
2.120	Warranties	41
2.121	Warranties and Representations	41
2.122	Warranty of Merchantability	42
2.123	Warranty of Fitness for a Particular Purpose	42
2.124	Warranty of Title	42
2.125	Equipment Warranty	42
2.126	Equipment to be New	43
2.127	Prohibited Products	43
2.128	Consequences for Breach	43
2.130	Insurance	43
2.13.1	Liability Insurance	43
2.13.2	Subcontractor Insurance Coverage	46
2.13.3	Certificates of Insurance	46
2.140	Indemnification	46
2.141	General Indemnification	46
2.142	Code Indemnification	46

2.143	Employee Indemnification	46
2.144	Patent/Copyright Infringement Indemnification	46
2.145	Continuation of Indemnification Obligations	47
2.146	Indemnification Procedures	47
2.150	Termination/Cancellation	48
2.151	Notice and Right to Cure	48
2.152	Termination for Cause	48
2.153	Termination for Convenience	48
2.154	Termination for Non-Appropriation	48
2.155	Termination for Criminal Conviction	49
2.156	Termination for Approvals Rescinded	49
2.157	Rights and Obligations upon Termination	49
2.158	Reservation of Rights	50
2.160	Termination by Contractor	50
2.161	Termination by Contractor	50
2.170	Transition Responsibilities	50
2.171	Contractor Transition Responsibilities	50
2.172	Contractor Personnel Transition	50
2.173	Contractor Information Transition	50
2.174	Contractor Software Transition	51
2.175	Transition Payments	51
2.176	State Transition Responsibilities	51
2.180	Stop Work	51
2.181	Stop Work Orders	51
2.182	Cancellation or Expiration of Stop Work Order	51
2.183	Allowance of Contractor Costs	51
2.190	Dispute Resolution	52
2.191	In General	52
2.192	Informal Dispute Resolution	52
2.193	Injunctive Relief	52
2.194	Continued Performance	52
2.200	Federal and State Contract Requirements	53
2.201	Nondiscrimination	53
2.202	Unfair Labor Practices	53
2.203	Workplace Safety and Discriminatory Harassment	53
2.204	Prevailing Wage	53
2.210	Governing Law	54
2.211	Governing Law	54
2.212	Compliance with Laws	54
2.213	Jurisdiction	54
2.220	Limitation of Liability	54
2.221	Limitation of Liability	54
2.230	Disclosure Responsibilities	54
2.231	Disclosure of Litigation	54
2.232	Call Center Disclosure	55
2.233	Bankruptcy	55
2.240	Performance	55
2.241	Time of Performance	55
2.242	Service Level Agreement (SLA)	56
2.243	Liquidated Damages	56
2.244	Excusable Failure	57
2.250	Approval of Deliverables	57
2.251	Delivery of Deliverables	57
2.252	Contractor System Testing	58
2.253	Approval of Deliverables, In General	58
2.254	Process for Approval of Written Deliverables	59
2.255	Process for Approval of Custom Software Deliverables	60
2.256	Final Acceptance	60

<u>2.260</u>	<u>Ownership</u>	61
	<u>2.261</u> <u>Ownership of Work Product by State</u>	61
	<u>2.262</u> <u>Vesting of Rights</u>	61
	<u>2.263</u> <u>Rights in Data</u>	61
	<u>2.264</u> <u>Ownership of Materials</u>	61
<u>2.270</u>	<u>State Standards</u>	61
	<u>2.271</u> <u>Existing Technology Standards</u>	61
	<u>2.272</u> <u>Acceptable Use Policy</u>	61
	<u>2.273</u> <u>Systems Changes</u>	62
	<u>2.274</u> <u>Electronic Receipt Processing Standard</u>	62
<u>2.280</u>	<u>Extended Purchasing Program</u>	62
	<u>2.281</u> <u>Extended Purchasing Program</u>	62
<u>2.290</u>	<u>Environmental Provision</u>	62
	<u>2.291</u> <u>Environmental Provision</u>	62
<u>2.300</u>	<u>Deliverables</u>	64
	<u>2.301</u> <u>Software</u>	64
	<u>2.302</u> <u>Hardware</u>	64
<u>2.310</u>	<u>Software Warranties</u>	64
	<u>2.311</u> <u>Performance Warranty</u>	64
	<u>2.312</u> <u>No Surreptitious Code Warranty</u>	64
	<u>2.313</u> <u>Calendar Warranty</u>	64
	<u>2.314</u> <u>Third-party Software Warranty</u>	65
	<u>2.315</u> <u>Physical Media Warranty</u>	65
<u>2.320</u>	<u>Software Licensing</u>	65
	<u>2.321</u> <u>Cross-License, Deliverables Only, License to Contractor</u>	65
	<u>2.322</u> <u>Cross-License, Deliverables and Derivative Work, License to Contractor</u>	65
	<u>2.323</u> <u>License Back to the State</u>	65
	<u>2.324</u> <u>License Retained by Contractor</u>	66
	<u>2.325</u> <u>Pre-existing Materials for Custom Software Deliverables</u>	66
<u>2.330</u>	<u>Source Code Escrow</u>	66
	<u>2.331</u> <u>Definition</u>	66
	<u>2.332</u> <u>Delivery of Source Code into Escrow</u>	66
	<u>2.333</u> <u>Delivery of New Source Code into Escrow</u>	67
	<u>2.334</u> <u>Verification</u>	67
	<u>2.335</u> <u>Escrow Fees</u>	67
	<u>2.336</u> <u>Release Events</u>	67
	<u>2.337</u> <u>Release Event Procedures</u>	67
	<u>2.338</u> <u>License</u>	67
	<u>2.339</u> <u>Derivative Works</u>	67
	<u>Glossary</u>	68
	<u>Attachment 1 – Service Level Agreement</u>	70
	<u>Attachment 2 – Hosting Environment</u>	74
	<u>Attachment 3 – ImageTrend Security and Disaster Recovery Process</u>	79
	<u>Attachment 4 – EDS Data Security Policies and Procedures</u>	84
	<u>Attachment 6 – Cost Tables</u>	112

Article 1 – Statement of Work (SOW)

1.000 Project Identification

1.001 PROJECT REQUEST

The State of Michigan (State), through the Department of Technology, Management & Budget (DTMB) in partnership with the Michigan Department of Community Health (MDCH) Emergency Medical Services (EMS) & Trauma Systems Section has issued this Contract for ongoing maintenance, hosting and services for the Michigan Emergency Medical Services Information System (MEMSIS).

The resulting Contract will be for time period of 4/1/2014 through 9/30/2019 with five one-year options to renew.

1.002 BACKGROUND

DCH Emergency Medical Services Mission Statement:

To protect and improve the health and well-being of Michigan citizens who require emergency medical services, through the administration of license requirements for EMS Operations and Vehicles, the oversight of local Medical Control Authorities and the development of regulatory policies and procedures which promote efficient program administration and safe care, treatment and transportation of the sick and injured.

The Emergency Medical Services Section is responsible for licensing over 800 life support agencies and over 3,000 life support vehicles. The Section approves local Medical Control Authorities (a hospital or group of hospitals) that provide community based pre-hospital emergency care oversight. Each county (or group of counties) is required to have such an Authority with the responsibility to establish policies, procedures and protocols focusing specifically on how pre-hospital emergency care will be carried out within their particular geographic area. The section also approves each of the 62 Authority's pre-hospital care policies, procedures and protocols prior to implementation. The Section is responsible to ensure that all life support agencies are in compliance with the communications standards prescribed under the State Medical Communications (MEDCOM) Requirements.

Under part 209 of the Public Health Code, the Michigan Department of Community Health is required to collect Emergency Medical Services data on a statewide basis. The MEMIS is a commercial-off-the-shelf (COTS) NEMSIS compliant application that enables state EMS agencies to securely collect, analyze and report on statewide EMS data. The software allows data to be collected through the use of a web-portal. The portal provides a secure method of collecting pre-hospital data, extracting existing data, and exporting or sharing data with other agencies and applications. Additionally, the software allows ambulance services to satisfy reporting requirements.

1.100 Scope of Work and Deliverables

1.101 IN SCOPE

The Contractor must provide the following services for the complete and successful support, maintenance and hosting of the Michigan Emergency Medical Services Information System (MEMSIS) and associated modules including the functionality required for the State's business operations.

This project consists of the following components:

- A. Maintenance and Support** - Maintenance is defined as repair or replacement services provided after the expiration of the warranty period necessary to identify and repair software malfunctions in order to return the system to its original operating condition. Maintenance also includes an agreement to provide an annual renewable software subscription to include future upgrades (both

major and minor revisions of the application) and ongoing Contractor product support, Help Desk and Technical support.

- B. Hosting**– Contractor hosted solution to include procuring, installing and maintaining application server(s) and other required hardware/software. The solution must include production, development and test/training environments. The development and test hardware/operating system environment will resemble the production environment. The State reserves the option to continue with the Contractor hosted solution or host within the State’s environment for the duration of the contract.
- C. Future Initiatives**– These projects will be determined at time of need and a separate work statement will be developed.

A more complete description of the supplies and/or services sought for this project is provided in Section 1.104, Work and Deliverables.

1.102 OUT OF SCOPE

The State is not seeking a new or replacement system.

1.103 ENVIRONMENT

The links below provide information on the State’s Enterprise information technology (IT) policies, standards and procedures which includes security policy and procedures, IT strategic plan, eMichigan web development and the State Unified Information Technology Environment (SUITE).

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. Contractors are expected to provide proposals that conform to State IT policies and standards. All services and products provided as a result of this Contract must comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response.

Enterprise IT Policies, Standards and Procedures:

<http://www.michigan.gov/dmb/0,1607,7-150-56355-107739--,00.html>

All software and hardware items provided by the Contractor must run on and be compatible with the MDTMB Standard Information Technology Environment. Additionally, the State must be able to maintain software and other items produced as the result of the Contract. Therefore, non-standard development tools may not be used unless approved by MDTMB. The Contractor must request, in writing, approval to use non-standard software development tools, providing justification for the requested change and all costs associated with any change. The MDTMB Project Manager must approve any tools, in writing, before use on any information technology project.

It is recognized that technology changes rapidly. The Contractor may request, in writing, a change in the standard environment, providing justification for the requested change and all costs associated with any change. The State’s Project Manager must approve any changes, in writing, and MDTMB, before work may proceed based on the changed environment.

Enterprise IT Security Policy and Procedures:

http://www.michigan.gov/documents/dmb/1310_183772_7.pdf

http://www.michigan.gov/documents/dmb/1310.02_183775_7.pdf

http://www.michigan.gov/documents/dmb/1325_193160_7.pdf

http://www.michigan.gov/documents/dmb/1335_193161_7.pdf

http://www.michigan.gov/documents/dmb/1340_193162_7.pdf

http://www.michigan.gov/documents/dmb/1350.10_184594_7.pdf

IT eMichigan Web Development Standard Tools:

http://www.michigan.gov/documents/som/Look_and_Feel_Standards_302051_7.pdf

The State Unified Information Technology Environment (SUITE):

Includes standards for project management, systems engineering, and associated forms and templates – must be followed: <http://www.michigan.gov/suite>

Current Technical Environment

Contractor must be able to securely maintain, support, enhance and host the MEMSIS using the below licensed software and technical environment to meet the needs of the State.

Current software system components include:

- EMS State Bridge
- Visual Informatics (Data Mining)
- Patient Registry (Trauma Bridge)

Technical Environment includes:

- Database: Microsoft SQL Server 08 R2 or greater
- Development Language: Microsoft .NET
- Development Framework: Microsoft .NET Framework 3.5 or greater
- Web Server: Microsoft IIS version 7.0 or greater
- Application Server: Windows Server 2008 R2 Standard Edition or greater
- Operating System: Microsoft Windows 2008 R2 or greater
- Reporting Tools: ImageTrend State Bridge™ Custom Reporting Module

The Contractor must remain current National EMS Information System (NEMSIS) compliant.

1.104 WORK AND DELIVERABLE

A. Software Maintenance and Support

The Contractor will supply software maintenance and support services that provide systems management as defined below for a flat-fixed annual cost aligned with the State's Fiscal Year. **Further details can be found in Attachment 1 – Service Level Agreement, Attachment 2 – Hosting Environment, Attachment 3 – ImageTrend Security and Disaster Recovery Process and Attachment 4 – EDS Data Security Policies and Procedures:**

- 1. System Maintenance Activities** – Contractor will provide Software maintenance. System Maintenance refers to regular and routine work performed by the Contractor on the MEMSIS. This includes any work required to correct defects in the system operation as required to meet Contract requirements. This also includes any routine file maintenance to update any information required for operation of the system such as data changes, constructing new edits, investigating batch job failures, investigating and correcting application defaults, repairing jobs run incorrectly, repairing problems due to system software failures, repairing problems due to operator or schedule error, rectifying problems due to web page, program, object, class, scripts, control language, or database errors, repairing security problems, repairing and restoring corrupted files, table structures, and databases, rectifying incorrect documentation, and repairing problems due to jobs run with incorrect data.
 - a. The Contractor will perform system maintenance.
 - b. All maintenance will be performed by qualified personnel who are familiar with the system.
 - c. The Contractor will provide backup maintenance resources.
 - d. The Contractor will provide the State access to regular database backup files

- e. The Contractor will provide for escalation of maintenance issues to ensure critical issues are resolved.
- f. The Contractor will provide remote diagnostic capabilities.
- g. The Contractor will provide one point of contact to report system malfunction whether malfunction is due to software or is of unknown origin. The Contractor will then be responsible for providing the appropriate remedy.
- h. The Contractor's annual renewable software subscription must include future upgrades (both major and minor revisions of the application)
- i. The Contractor must coordinate new releases and other changes with the State prior to implementation.
- j. The Contractor must maintain support for the customized medical control authority access.
- k. The Contractor shall offer a live test and training environment alongside of the functioning service. This test and training environment will be loaded with mock data and used by EMS & Trauma Systems Section for training and exercise purposes.
- l. Contractor will provide the following services for the system:
 - i. **Error Correction.** If an error occurs the Contractor shall use commercially reasonable efforts to correct or provide a working solution for the problem. The State will be notified upon discovery of any error and promptly when corrections made.
The State will be provided with information on software problems encountered at other locations, along with the solution to those problems, when such information is relevant to State software
 - ii. **Material Defects.** The Contractor will notify the State of any material errors or defects in the deliverables known, or made known to the Contractor from any source during the Contract term that could cause the production of inaccurate or otherwise materially incorrect, results and shall initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects..
 - iii. **Updates.** All new releases and bug fixes (collectively referred to as "Changes") for any software deliverable developed or published by Contractor and made generally available to its other customers at no additional charge will be provided to the State at no additional charge.

2. Help Desk Support

Contractor must provide a toll free support telephone number 24x365x7 for all users utilizing the MEMSIS. The Contractor must provide on-call staff available 24 hours per day. Internet support and e-mail is also acceptable. The Contractor will provide access to online education materials for all contracted products. The Contractor's Support Team must be available Monday through Friday from 8:00 am to 5:00 pm EST. The response time during business hours are as follows.

Severity Level	Examples of each Severity Level:	Notification Acknowledgement: ImageTrend Return Call to Licensee after initial notification of an Error	Action Expectation: Anticipated Error resolution notification after ImageTrend Return Call to Licensee of Notification Acknowledgement of an error.
Severity 1 – Critical	<ul style="list-style-type: none"> - Complete shutdown or partial shutdown of one or more Software functions - Access to one or more Software functions not available - Major subset of Software 	Within one (1) hour of initial notification during business hours or via support@imagnetrend.com or Support Desk with critical subject status.	Six hours

	application impacted		
Severity 2 – Non-Critical	- Minor subsystem failure -Data entry or access impaired on a limited basis – usually can be delegated to local client contact as a first level or response for resolution – usually user error (i.e. training) or forgotten passwords	Within four (4) hours of initial notification	24 Business hours
Severity 3 – Non-essential	- System operational with minor issues; suggested enhancements as mutually agreed upon – typically covered in next version release as mutually agreed upon.	Same day or next business day of initial notification	Next Release

3. Adaptive and Preventive Maintenance Activities

- a. Adaptive and preventive maintenance addresses upgrades to the system due to technical changes to system components to keep the system maintainable, including the following services:
 - i. Upgrades or patches of the application server, Windows components, operating system, or other system and application software.
 - ii. Software modifications and upgrades necessary because of expiring third party Contractor support.
 - iii. Hardware, database, or application conversions that do not modify user functionality.
 - iv. One-time loads or reformats of user data.
 - v. Report distribution changes.
- b. The changes should be transparent to the end user. The Contractor will provide Release Notes with all system upgrades/updates.
- c. Adaptive release changes will be performed in a quarterly patch release.
- d. For major upgrades requiring a more significant amount of time to develop, test, and implement, the changes should be completed as part of a development release or a quarterly release. Any major release which may require an upgrade to the server/desktop operating systems or third party software utilized as part of the MEMEIS must be documented and provided to the State three months prior to implementation to ensure all requirements can be obtained.
- e. Application Repair –Contractor must offer patches or fixes to acknowledged issues of the MEMEIS within an acceptable timeframe as mutually agreed to by the State and Contractor.

4. Performance Maintenance Activities – assist State staff in performance maintenance activities to improve the performance of the application.

- a. Performance maintenance includes the following services:
 - ii. Improve the performance, maintainability, or other attributes of an application system.
 - iii. Data table restructuring.
 - iv. Data purges and or archiving to reduce/improve data storage.
 - v. Run time improvements.
 - vi. Replace utilities to reduce run time.
 - vii. Potential problem correction.
 - viii. Data set expansions to avoid space problems.

5. **Documentation Update**

Documentation (electronic) for scheduled software releases to include changes or enhancements to the existing system at no additional cost to the State. Documentation must include:

- For each software release the Contractor must provide release notes to the State detailing the changes/upgrades that are included in the software release. The release notes must identify reported bug fixes and new functionality added by the Contractor.
 - The Contractor will provide the State electronic access to obtain current and future System Administrator Manual or guide and a User Manual which will cover all functions of the current and future contractor's software that is installed and supports the MEMIS. The Contractor will provide a Word version of the Guides and Manuals which the State can customize to detail the MEMIS as installed and configured for the State. If the State would like the Contractor to provide the customization, they can be provided at an additional fee. The State must have unlimited reproduction rights to the manuals for management purposes.
 - The Contractor will provide updated Systems Administrator manuals and User Manuals for major releases that include new functionality in the MEMIS.
- Security Changes- Any changes to user access or administrator access security will be provided in the release notes.

B. Hosting Requirements

The Contractor will supply hosting services as defined below for a flat-fixed annual cost aligned with the State's Fiscal Year.

- i. The Contractor will provide the following for hosting solution during the Contract period:
 - a. Software - Apply hot-fixes and service packs as needed to address anomalies and security concerns. Software support applies to third party software including operating system, back ups, antivirus software, and any application software as related to the hosting services and provided by the Contractor.
 - b. Hardware - Apply Firmware and Bios updates as needed to address anomalies and security concerns. Updates are provided by the hardware Contractor and must be tested internally prior to install.
 - c. Server - Standard hardware and software maintenance as listed above to ensure reliability and optimal performance. This maintenance will occur weekly, monthly and quarterly depending on tasks.
 - d. Firewall - Must be deployed using current industry best practice model. Logs are to be monitored and maintained to ensure reliability and security.
 - e. Anti-Viral – Must provide a reliable industry-standard anti-virus system. Virus definition file maintenance and updates must be done daily to ensure complete virus protection. System must have weekly proactive scans during off peak periods.
 - f. Power Systems and Infrastructure – The facility must meet or exceed the Uptime Institute Tier 3 Data Facility standards. (<http://www.uptimeinstitute.org/>) Primary infrastructure systems must be monitored and redundant, with battery and generator backup power. Circuit load must be checked regularly to ensure reliable power to systems.
 - g. Internet Connectivity - Must be redundant connections with burstable bandwidth support. The connectivity must automatically adjust to handle increased load during an alert.
 - h. Telephone Lines - Service must be maintained and operational tested at regular intervals.
 - i. Encryption & Server Certificates - Must be registered and installed on all web servers. All web traffic transferred from MEMIS to the public internet must be encrypted.
 - j. Domain Names – Must be registered for both the primary and alternate sites. Domain Name Services for all public facing web servers and all internal systems must be maintained and redundant.

- k. Systems & Data Backup - Must occur nightly. Data must be transferred to tape or other portable media, removed from the data center, and stored at a secure site.
- l. Systems Failover – Failover to an alternate site is to be available at all times with little or no notice. In order to maintain uptime, critical services must be transferred in the event of a prolonged outage at the primary site. The alternate site must be located geographically separated from the primary site.
- m. Server Computers – Increased hardware capacity may be needed to deal with system expansion and performance needs. The site infrastructure hosting the systems must have the capacity to add additional servers and meet power needs.
- n. Infrastructure Hardware - Should be added as needed to deal with system expansion and performance needs. The site infrastructure hosting the systems must have the capacity to add additional equipment and meet power needs.
- o. Power Systems as Needed - The site infrastructure hosting the systems must have the capacity to add additional power to meet growing needs.
- p. The MEMIS must be fully available 99.9% of the time during normal business hours of 8AM to 5PM EST on business days and also available on-call during non-business hours to support the hosted infrastructure as well as application software.
- q. Performance and Capacity Management
 - Monitor, collect, and analyze Server utilization data for CPU, memory, and disk space;
 - Compile configuration data and usage patterns;
 - Monitor Server performance;
 - Establish thresholds and exception reporting procedures;
 - Perform tuning based on available performance data;
 - Review Server capacity trends;
 - With the State's assistance, establish a schedule for Contractor's performance of Server maintenance (for example, virus and malicious software detection, backup, disk space cleanup) and for implementing modifications and enhancements to the Web Hosting Environment so as to minimally impact availability of the Web Hosting Environment;
 - Fire detection and suppression a system for early detection of fires and suppression in a manner that does not damage state equipment
 - Air conditioning monitored facilities to control for temperature and humidity
 - Facility monitoring for electrical and mechanical failures, fire detection, and leak detection
 - Support services including system and network monitoring of backbone routers, WAN interfaces, routers, switches, and servers
 - Network problem detection, tracking, and resolution process
- r. Security Management
 - Define access controls for the Web Hosting Environment;
 - Monitor the Web Hosting Environment for unauthorized access;
 - Notify the State in accordance with the security procedures specified in the Contractor's Security Guidelines if the Contractor detects a security violation;
 - Follow the procedures specified in the Contractor Security Guidelines for logging, alarming and reporting of security violations;
 - Provide and maintain virus and malicious software avoidance, detection, and elimination software for Servers;
 - Conduct periodic security reviews;
 - Validate the correct use of logical control features such as time-out password screens and password and logon administration;
 - Physical security of the hosting location 24/7 and 365 day (monitored)
 - Controlled access to facilities during business, including logged access by time and date
 - Report access rights for State approval
 - State requires access to regular database backup files
- s. Storage Management Services

- Maintain and implement database backup and restore processes and procedures to attempt to restore Servers following outages or corruption;
 - Conduct routine backup and restore procedures so as not to adversely impact scheduled operations, including regular backups from disk to tape for the Servers during nightly backup windows;
 - Assist the State in the restoration of files deleted or corrupted.
 - The Web Hosting Environment will provide daily incremental backup of all Servers with the ability to restore to the most recent backup;
 - Backup and restore Content;
- t. Reports
1. Server Availability Reports
 - Outage Summary Report
 - Outage by Server Report
 - i. The start and end time of each outage;
 - ii. The duration of the outage;
 - iii. The IP address experiencing the outage;
 - iv. Reason for the outage, if known;
 - v. Description of the actions required to resolve the outage problem;
 - vi. Total time the Server was unavailable; and
 - vii. Name of the Contractors technical team member responsible for resolving the problem.
 2. Performance and Capacity Reports - graphical summary report contains a line graph and a bar chart showing the percentage of Servers in which utilization of a particular resource (i.e., CPU, memory, disk space) was either red, yellow, or green.
 3. Capacity Summary Report - contains a bar chart and a table showing the percentage of Servers in which utilization of a particular resource (i.e., CPU, memory, and disk space) was either red, yellow, or green as defined above. There is also a bar chart and table that show overall resource utilization. The report shows approximately 24 months of data.
- u. Hardware –

The Contractor will meet the following Standards:

- Connection: Minimum uptime: 99.9%.
- System availability: 24x7x365.
- An Uninterruptible Power Supply must protect all servers.
- All servers should have dual network cards for fail-over.
- All servers must be located in a security locked room accessible only by authorized personnel
- All outside connections must pass through an approved State of Michigan Firewall.
- All servers are protected by State of Michigan approved Anti-Virus software.
- All servers must pass a State of Michigan approved vulnerability scan, with remediation in 48 hours.
- All servers have their OS upgraded upon release with ample time allowed for bug fixes.
- The Contractors proposed solution must include the following environments:
 - Development
 - Testing
 - Live Production

The Contractor may propose combining environments; however, the Live Production environment must be physically separate from the other environments.

Redundancy shall be designed into the system to handle failure situations and make system maintenance possible without experiencing downtime. Server redundancy is not required; however backup procedures minimize the chance of data loss in the event of a hardware failure. In the event of a prolonged outage due to hardware failure, other

servers are available to temporarily run the application. Contractor may provide additional alternatives that will meet the redundancy requirement and will provide a cost savings to the State.

ii. **Hosting & Site Security**

Physical system security is paramount. All systems must be housed within a secured facility and kept within a secured cabinet or cage. The facility must track and control all access entering and exiting the building and server room, as well as having physical security systems and video surveillance.

- a. Location of Work Requirements - The work is to be performed, completed, and managed in (2) geographically separated level (3) secure data centers. The data centers must be located in different geographic regions of the United States e.g. California and Texas.
- b. Security and Confidentiality Requirements
 - i. All sites must be secured from Internet, Intranet or On-Site intrusions or attacks.
 - ii. All equipment must be kept secure from On-Site intrusions or attacks.
 - iii. All data must be secured from Internet, Intranet or On-Site intrusions or attacks.
 - iv. All Internet based data transmission must be encrypted.

iii. **Disaster Recovery**

Contractor and the State recognize that the State provides essential services in times of natural or man-made disasters. Therefore, except as so mandated by Federal disaster response requirements, Contractor personnel dedicated to providing Services/Deliverables under this Contract will provide the State with priority service for repair and work around in the event of a natural or manmade disaster.

The Contractor will provide a disaster recovery strategy document and include at minimum:

- The strategy to recover to a known state & resume after a site-loss disaster
- The ability to recover on-line transactions since the last backup in a non-site-loss disaster
- An annual demonstration of the ability to recover full functionality to another site
- Off-site transport of system and database backups

The Contractor must provide a document indicating the strategy to maintain system availability in the event of the loss of one or more system components.

Security – In addition to abiding with the disaster recovery and back up process, the Contractor must abide to the security requirements for all of the IT environments being hosted by the Contractor.

C. Future Initiatives

The Contractor will provide an as-needed reserve bank for future software licenses/modules, development or configuration activities, modifications, product enhancements, or work that does not fall under maintenance support as defined in the Contract. The State is not committed to use any of the reserve bank. The State reserves the right to add more to the reserve bank.

Future initiatives must be dependent upon mutually agreed statement(s) of work between the Contractor and the State of Michigan. Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a statement of work until authorized via a purchase order issued against this Contract.

Software

The State reserves the right to purchase additional software licenses/modules to support the State's MEMIS system operations throughout the term of this contract.

Services

The State reserves the right to purchase technical services to support the State's MEMIS system operations throughout the term of the Contract on an as-needed basis.

This reserve bank may be for future services and/or products to meet new requirements that may result from any or all of the following examples:

- A. New State policy requirements,
- B. New Federal regulations, or
- C. New technology requested by the State.

The reserve bank of hours may be used for:

- A. New Development - Contractor may provide the ability for new development work of the software.
- B. Interoperability Development with Other Applications - Contractor may provide the ability to request integrations or interoperability with other products or services of the software.
- C. System Interface Adjustments & New Interfaces – Contractor may provide the ability to request changes or customizations to the application user interface of the software.

The Contractor must be able to respond with costs and timelines to all requests to modify the MEMIS system to meet future needed functionality. Future enhancements must be dependent upon mutually agreed upon statement(s) of work between the Contractor and the State of Michigan. Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a statement of work until authorized via a purchase order issued against this contract.

Each Statements of Work will include:

1. Background
2. Project Objective
3. Scope of Work
4. Deliverables
5. Acceptance Criteria
6. Project Control and Reports
7. Specific Department Standards
8. Cost/Rate
9. Payment Schedule
10. Project Contacts
11. Agency Responsibilities
12. Location of Where the Work is to be performed
13. Expected Contractor Work Hours and Conditions

1.200 Roles and Responsibilities

1.201 CONTRACTOR STAFF, ROLES, AND RESPONSIBILITIES

A. Contractor Staff

The Contractor will provide sufficient qualified staffing to satisfy the deliverables of this Article 1 Statement of Work. Contractor must provide a list of all subcontractors, including firm name, address, contact person, and a complete description of the work to be contracted. Include descriptive information concerning subcontractor's organization and abilities.

The contractor must replace all employees whose work was found to be unsatisfactory as determined by the DTMB project manager within five (5) business days of notification.

The Contractor will provide, and update when changed, an organizational chart indicating lines of authority for personnel involved in performance of the Contract and relationships of this staff to other programs or functions of the firm. This chart must also show lines of authority to the next senior level of management and indicate who within the firm will have prime responsibility and final authority for the work.

Single Point of Contact (SPOC)

The Contractor will identify a SPOC. The duties of the SPOC shall include, but not be limited to:

- supporting the management of the Contract,
- facilitating dispute resolution, and
- advising the State of performance under the terms and conditions of the Contract.

The State reserves the right to require a change in the current SPOC if the assigned SPOC is not, in the opinion of the State, adequately serving the needs of the State.

Key Personnel

The State reserves the right to designate Key Personnel to be provided by the Contractor, as part of individual SOW's. The State reserves the right to interview all Key Personnel and to approve their assignment.

B. On Site Work Requirements

1. Location of Work

The work is to be performed, completed, and managed at the Vendors location. NO work will be performed offshore.

2. Hours of Operation:

- a. Normal State working hours are 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, with work performed as necessary after those hours to meet project deadlines. No overtime will be authorized or paid.
- b. The State is not obligated to provide State management of assigned work outside of normal State working hours. The State reserves the right to modify the work hours in the best interest of the project.
- c. Contractor shall observe the same standard holidays as State employees. The State does not compensate for holiday pay.

3. Travel:

- a. No travel or expenses will be reimbursed, unless formally agreed upon by the State in advanced. This includes travel costs related to training provided to the State by Contractor.
- b. The State is not responsible for providing the use of vehicles for the Contractor.
- c. The State is not responsible for providing housing accommodations to the Contractor.

4. Additional Security and Background Check Requirements:

Contractor must present certifications evidencing satisfactory Michigan State Police Background checks ICHAT and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

1.202 STATE STAFF, ROLES, AND RESPONSIBILITIES

The State will provide the following resources for the Contractor's on-site use, as determined for a specific engagement, through individual Statements of Work. These may include:

- Work space
- Minimal clerical support

Desk
 Telephone
 PC workstation
 Printer
 Access to copiers and fax machine
 Other. Specify: deemed necessary by DTMB to perform tasks identified in this Contract.

Note: The State reserves the right to inspect and scan any equipment supplied by the Contractor that will be connected to the State's network.

The Contractor is responsible for the return of all State issued equipment in the same condition as when provided by the State, reasonable wear and tear expected, upon Contractor staff release from the project.

The State project team will consist of DTMB and Agency project managers:

State Program Manager-

MDTMB and DCH will provide a Program Manager who will be responsible for overseeing all services performed under the Contract and coordinating with the. The State's Program Managers will provide the following services:

- Supporting the management of the Contract.
- Resolve project issues in a timely manner
- Review project plan, status, and issues
- Resolve deviations from project plan
- Provide acceptance sign-off
- Utilize change control procedures
- Ensure timely availability of State resources
- Make key implementation decisions, as identified by the Contractor's project manager, within 48-hours of their expected decision date.
- Provide State facilities, as needed
- Coordinate the State resources necessary for the project
- Facilitate coordination between various external Contractors
- Facilitate communication between different State departments/divisions
- Provide acceptance and sign-off of deliverable/milestone
- Review and sign-off of timesheets and invoices
- Resolve project issues
- Escalate outstanding/high priority issues
- Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
- Document and archive all important project decisions
- Arrange, schedule and facilitate State staff attendance at all project meetings.
- Escalate outstanding/high priority issues
- Utilize change control procedures
- Conduct regular and ongoing review of the program to confirm that it meets original objectives and requirements
- Document and archive all important program decisions
- Facilitate communication with State project and operational staff.

Name	Agency/Division	Title
George Hamel	MDTMB	Program Manager
Marvin Helmker	MDCH	EMS Manager

1.300 Project Plan

1.301 PROJECT PLAN MANAGEMENT

Project Plan

Specific project plans requirements may be defined within individual Statements of Work.

Contract Kick-Off Meeting

Upon 14 calendar days from execution of the Contract, the Contractor may be required to attend an orientation meeting to discuss the content and procedures of the Contract. The meeting will be held in Lansing, Michigan, at a date and time mutually acceptable to the state and the Contractor. The state shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Performance Review Meetings

The State may require the Contractor to attend meetings as needed, to review the Contractor's performance under the Contract. The meetings will be held in Lansing, Michigan or by teleconference, as mutually agreed by the State and the Contractor. The State shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Program Control

1. The Contractor will carry out this program under the direction and control of DTMB. The DTMB project manager will review progress reports and will review and approve payments.
2. The Contractor will manage projects in accordance with the State Unified Information Technology Environment (SUITE) methodology, which includes standards for project management, systems engineering, and associated forms and templates which is available at <http://www.michigan.gov/suite>
 - a. Contractor will use an automated tool for planning, monitoring, and tracking the Contract's progress and the level of effort of any Contractor personnel spent performing Services under the Contract. The tool shall have the capability to produce:
 - i. Staffing tables with names of personnel assigned to Contract tasks.
 - ii. Project plans showing tasks, subtasks, deliverables, and the resources required and allocated to each (including detailed plans for all Services to be performed within the next sixty (60) calendar days, updated semi-monthly).
 - iii. Updates must include actual time spent on each task and a revised estimate to complete.
 - iv. Graphs showing critical events, dependencies and decision points during the course of the Contract.
 - b. Any tool(s) used by Contractor for such purposes must produce information of a type and in a manner and format that will support reporting in compliance with the State standards.
3. The DTMB project manager shall have contact as needed with individual Contract employees for the purpose of reviewing progress and providing necessary guidance in solving problems which arise. The objective of this step is to ensure that the DTMB project manager is promptly informed of issues and risks that confront the Contractor employees throughout the Contract.
4. All project assignments and tasks will be undertaken only upon the prior written authorization of the DTMB project manager. The written authorization will include a definition of tasks, deliverables, estimated hours, fixed unit price per hour for each personnel classification, extended price for each personnel classification, maximum price for the authorization, and authorization expiration date. Hours authorized for each task may not be exceeded without a change order issued by the DTMB project manager. If the Contractor employees identify tasks that they anticipate may exceed the estimated amounts, they should notify the DTMB project manager so that any work stoppage may be avoided.

1.302 REPORTS

Specific reporting requirements will be defined within individual Statements of Work. Reporting formats must be submitted to the State's Project Manager for approval within 10 business days after the execution of the Contract. Once both parties have agreed to the format of the report, it shall become the standard to follow for the duration of the Contract. At minimum the status reports shall include:

- Dates of the week covered (daily breakdown by project)
- Contractor name

- DTMB manager name
- Contract name
- P.O. number
- For each project on which the resource worked during the week:
 - Project name
 - Work authorization number
 - Number of hours worked on the project for each business day of the week
 - Total number of hours worked on the project during the week
- Total number of hours being billed for the week
- DTMB and/or project manager signature and date
- Contractor signature and date

The status report will include the following items for which the resource has worked:

- Project name
- Milestones/deliverables completed
- Tasks accomplished
- Next steps
- Potential issues/risks

1.400 Project Management

1.401 ISSUE MANAGEMENT

An issue is an identified event that if not addressed may affect schedule, scope, quality, or budget.

The Contractor shall maintain an issue log for issues relating to the provision of services under this Contract. The issue management log must be communicated to the State's Project Manager on an agreed upon schedule, with e-mail notifications and updates. The issue log must be updated and must contain the following minimum elements:

1. Description of issue.
2. Issue identification date.
3. Responsibility for resolving issue.
4. Priority for issue resolution (to be mutually agreed upon by the State and the Contractor).
5. Resources assigned responsibility for resolution.
6. Resolution date.
7. Resolution description.

Once the Contractor or the State has identified an issue, the Contractor shall follow these steps:

1. Immediately communicate the issue in writing to the State's Project Manager.
2. The Contractor will log the issue into an issue tracking system.
3. Identify what needs to be done and resources needed to correct the issue.
4. Receive approval from the State's Project Manager for appropriate action.
5. Keep State's Project Manager and appropriate parties informed on status of issue based on frequency established by the State's Project Manager.
6. At least monthly provide a listing of all issues with their current status, deadlines to correct and actual dates of completion that have occurred to the State's Project Manager.

Issues shall be escalated for resolution from level 1 through level 2, as defined below:

- Level 1 – Project Manager
- Level 2 – Contract Compliance Inspector

1.402 RISK MANAGEMENT

A risk is an unknown circumstance or event that, if it occurs, may have a positive or negative impact on the project.

The Contractor is responsible for establishing a risk management plan and process, including the identification and recording of risk items, prioritization of risks, definition of mitigation strategies, monitoring of risk items, and periodic risk assessment reviews with the State.

A risk management plan format shall be submitted to the SOM for approval within twenty (20) business days after Contract signing. The risk management plan will be developed during the initial planning phase of the project, and be in accordance with the SOM PMM methodology. Once both parties have agreed to the format of the plan, it shall become the standard to follow for the duration of the Contract. The plan must be updated bi-weekly, or as agreed upon.

The Contractor shall provide the tool to track risks. The Contractor will work with the SOM and allow input into the prioritization of risks.

The Contractor is responsible for identification of risks for each phase of the project. Mitigating and/or eliminating assigned risks will be the responsibility of the Contractor. The State will assume the same responsibility for risks assigned to them.

1.403 CHANGE MANAGEMENT

Change management is defined as the process to communicate, assess, monitor, and control all changes to system resources and processes. The State also employs change management in its administration of the Contract.

If a proposed Contract change is approved by the Agency, the Contract Administrator will submit a request for change to the Department of Technology, Management and Budget, Procurement Buyer, who will make recommendations to the Director of DTMB-Procurement regarding ultimate approval/disapproval of change request. If the DTMB Procurement Director agrees with the proposed modification, and all required approvals are obtained (including State Administrative Board), the DTMB-Procurement Buyer will issue an addendum to the Contract, via a Contract Change Notice. **Contractors who provide products or services prior to the issuance of a Contract Change Notice by the DTMB-Procurement risk non-payment for the out-of-scope/pricing products and/or services.**

The Contractor must employ change management procedures to handle such things as "out-of-scope" requests or changing business needs of the State while the migration is underway.

The Contractor will employ the change control methodologies to justify changes in the processing environment, and to ensure those changes will not adversely affect performance or availability.

1.500 Acceptance

1.501 CRITERIA

1. The services will be accepted in accordance with the requirements of the Contract.
2. State will review maintenance requests within a mutually agreed upon timeframe from.
 - a. Approvals will be written and signed by State Project Managers.
 - b. Unacceptable issues will be documented and submitted to the Contractor.
 - c. After issues are resolved or waived, the Contractor will resubmit a revised Maintenance Request for Approval of Services within 10 days.
3. The Contractor will maintain the tools and connectivity installed, in compliance with DTMB standards, to properly support and monitor the application.
4. State will review a Request for Approval of Services within a mutually agreed upon timeframe from completion or implementation.

- a. Approvals will be written and signed by State Project Managers.
 - b. Unacceptable issues will be documented and submitted to the Contractor.
 - c. After issues are resolved or waived, the Contractor will resubmit a Request for Approval of Services for approval within 30 days of receipt.
5. State will review migrated and configured data within a mutually agreed upon timeframe from completion.
- a. Approvals will be written and signed by State Project Managers.
 - b. Unacceptable issues will be documented and submitted to the Contractor.
 - c. After issues are resolved or waived, the Contractor will resubmit a request for approval within 30 days of receipt.
6. The Contractor has the tools and connectivity installed, in compliance with DTMB standards, to properly support and monitor the application.
7. Specific acceptance criteria for software enhancements will be included in each Statement of Work.
8. The following criteria apply to software enhancement deliverables:
- a. Beta software is not accepted as final deliverable.
 - b. MDTMB will review the software enhancements for acceptance of functionality, usability, installation, performance, security, standards compliance, backup/recovery and operation. Approvals will be written and signed by Agency/MDTMB Project Manager as identified in applicable statement of work. Unacceptable issues will be documented and submitted to the Contractor. After issues are resolved or waived, the Contractor will resubmit software for approval.
 - c. Software enhancements are installed and configured in appropriate environment (e.g. development, test, pre-live, live). Contingency plans and de-installation procedures and software are provided by Contractor and approved by the Agency/MDTMB Project Managers as identified in applicable statement of work.
 - d. Contractor will successfully test software enhancements in the development environment before moving the enhancement to the test and pre-live environments for final software testing by Agency/MDTMB. Approvals will be written and signed by Agency/MDTMB Project Managers.
 - e. Unacceptable issues will be documented and submitted to the Contractor. After issues are resolved or waived, the Contractor will resubmit test software, data and results for approval. Only after successful State testing in the test and pre-live area will the enhancement be implemented in the production environment. This implementation should occur at an agreed upon time during non business hours, such as late evenings or weekends.

1.502 FINAL ACCEPTANCE

Final acceptance criteria for deliverables will be identified in each individual project SOW.

1.600 Compensation and Payment

1.601 COMPENSATION AND PAYMENT

Method of Payment

Annual payment shall be made on a firm-fixed cost basis for Maintenance and Hosting Support that aligns with the State's Fiscal Year dates.

For future deliverables, the State reserves the right to determine whether payment shall be made on a firm fixed-hourly rate basis, or on completion and acceptance of specified deliverables or milestones. The parties agree that the Services/Deliverables to be rendered by Contractor pursuant to the Contract (and any future amendments of it) will be defined and described in detail in a Statement of Work.

Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a Statement of Work until authorized via a purchase order issued against the Contract.

Payments will be paid no more than monthly.

The Contractor will not be paid for any costs attributable to corrections of any errors or omissions that have been determined by the DTMB Project Manager to be caused by the Contractor.

Prices quoted will be firm for the entire length of the Contract. For any options to renew (see Section 2.002), prices may not be increased by more than the previous year's Consumer Price Index (CPI) or 3%, whichever is lower.

The Contractor will be required to submit an Administrative Fee (see Section 2.031) on all payments remitted under the Contract.

Notification of Price Reductions

If Contractor reduces its prices for any of the services during the term of the Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send notice to the State's DTMB Procurement Buyer with the reduced prices within fifteen (15) Business Days of the reduction taking effect.

Travel

The State will not pay for any travel expenses, including hotel, mileage, meals, parking, etc. Travel time will not be reimbursed.

Issuance of Purchase Orders (PO)

Contractor shall not be obliged or authorized to commence any work orders until authorized via a PO issued against this Contract. Contractor shall perform in accordance with this Contract, including the SOWs and Purchase Orders executed under it.

Invoicing

Contractor will submit properly itemized invoices to

DTMB – Financial Services
Accounts Payable
P.O. Box 30026
Lansing, MI 48909
or
DTMB-Accounts-Payable@michigan.gov

Invoices must provide and itemize:

- Contract number;
- Purchase Order number
- Contractor name, address, phone number, and Federal Tax Identification Number;
- Description of service;
- Date(s) of delivery;
- Cost/Rate;
- Total invoice price; and
- Payment terms, including any available prompt payment discount.

Incorrect or incomplete invoices will be returned to Contractor for correction and reissue.

1.602 HOLDBACK

The State shall have the right to hold back an amount equal to percent 10% of all amounts invoiced by Contractor for specified deliverables for future enhancements. The amounts held back shall be released to Contractor after the State has granted Final Acceptance.

Article 2, Terms and Conditions

2.000 Contract Structure and Term

2.001 CONTRACT TERM

This Contract is for a period beginning April 1st, 2014 through September 30th 2019. All outstanding Purchase Orders must also expire upon the termination for any of the reasons listed in **Section 2.150** of the Contract, unless otherwise extended under the Contract. Absent an early termination for any reason, Purchase Orders issued but not expired, by the end of the Contract's stated term, shall remain in effect for the balance of the fiscal year for which they were issued.

2.002 OPTIONS TO RENEW

This Contract may be renewed in writing by mutual agreement of the parties not less than 30 days before its expiration. The Contract may be renewed for up to five (5) additional one (1) year periods.

2.003 LEGAL EFFECT

Contractor accepts this Contract by signing two copies of the Contract and returning them to the DTMB-Procurement. The Contractor shall not proceed with the performance of the work to be done under the Contract, including the purchase of necessary materials, until both parties have signed the Contract to show acceptance of its terms, and the Contractor receives a contract release/purchase order that authorizes and defines specific performance requirements.

Except as otherwise agreed in writing by the parties, the State shall not be liable for costs incurred by Contractor or payment under this Contract, until Contractor is notified in writing that this Contract or Change Order has been approved by the State Administrative Board (if required), signed by all the parties and a Purchase Order against the Contract has been issued.

2.004 ATTACHMENTS & EXHIBITS

All Attachments and Exhibits affixed to any and all Statement(s) of Work, or appended to or referencing this Contract, are incorporated in their entirety and form part of this Contract.

2.005 ORDERING

The State must issue an approved written Purchase Order, Blanket Purchase Order, Direct Voucher or Procurement Card Order to order any Services/Deliverables under this Contract. All orders are subject to the terms and conditions of this Contract. No additional terms and conditions contained on either a Purchase Order or Blanket Purchase Order apply unless they are specifically contained in that Purchase Order or Blanket Purchase Order's accompanying Statement of Work. Exact quantities to be purchased are unknown; however, the Contractor will be required to furnish all such materials and services as may be ordered during the Contract period. Quantities specified, if any, are estimates based on prior purchases, and the State is not obligated to purchase in these or any other quantities.

2.006 ORDER OF PRECEDENCE

The Contract, including any Statements of Work and Exhibits, to the extent not contrary to the Contract, each of which is incorporated for all purposes, constitutes the entire agreement between the parties with respect to the subject matter and supersedes all prior agreements, whether written or oral, with respect to the subject matter and as additional terms and conditions on the purchase order must apply as limited by **Section 2.005**.

In the event of any inconsistency between the terms of the Contract and a Statement of Work, the terms of the Statement of Work shall take precedence (as to that Statement of Work only), provided, however, that a Statement of Work may not modify or amend the terms of the Contract. The Contract may be modified or amended only by a formal Contract amendment.

2.007 HEADINGS

Captions and headings used in the Contract are for information and organization purposes. Captions and headings, including inaccurate references, do not, in any way, define or limit the requirements or terms and conditions of the Contract.

2.008 FORM, FUNCTION & UTILITY

If the Contract is for use of more than one State agency and if the Deliverable/Service does not meet the form, function, and utility required by that State agency, that agency may, subject to State purchasing policies, procure the Deliverable/Service from another source.

2.009 REFORMATION AND SEVERABILITY

Each provision of the Contract is severable from all other provisions of the Contract and, if one or more of the provisions of the Contract is declared invalid, the remaining provisions of the Contract remain in full force and effect.

2.010 Consents and Approvals

Except as expressly provided otherwise in the Contract, if either party requires the consent or approval of the other party for the taking of any action under the Contract, the consent or approval must be in writing and must not be unreasonably withheld or delayed.

2.011 NO WAIVER OF DEFAULT

If a party fails to insist upon strict adherence to any term of the Contract then the party has not waived the right to later insist upon strict adherence to that term, or any other term, of the Contract.

2.012 SURVIVAL

Any provisions of the Contract that impose continuing obligations on the parties, including without limitation the parties' respective warranty, indemnity and confidentiality obligations, survive the expiration or termination of the Contract for any reason. Specific references to survival in the Contract are solely for identification purposes and not meant to limit or prevent the survival of any other section

2.020 Contract Administration

2.021 ISSUING OFFICE

This Contract is issued by the Department of Technology, Management & Budget, Procurement, the DTMB Customer Services and the Michigan Department of Transportation (MDOT) (collectively, including all other relevant State of Michigan departments and agencies, the "State"). DTMB-Procurement is the sole point of contact in the State with regard to all procurement and contractual matters relating to the Contract. The DTMB-Procurement Contract Administrator for this Contract is:

Whitnie Zuker
Buyer
Procurement
Department of Technology, Management & Budget
Mason Bldg, 2nd Floor
PO Box 30026

Lansing, MI 48909
zuckerw@michigan.gov
517-335-5306

2.022 CONTRACT COMPLIANCE INSPECTOR

The Director of DTMB-Procurement directs the person named below, or his or her designee, to monitor and coordinate the activities for the Contract on a day-to-day basis during its term. **Monitoring Contract activities does not imply the authority to change, modify, clarify, amend, or otherwise alter the prices, terms, conditions and specifications of the Contract. DTMB-Procurement is the only State office authorized to change, modify, amend, alter or clarify the prices, specifications, terms and conditions of this Contract.** The Contract Compliance Inspector for this Contract is:

TBD

2.023 PROJECT MANAGER

The following individual will oversee the project:

Marvin Helmker, EMS Manager
EMS Section
Department of Community Health
Capitol View Building, 6th Floor
Lansing, MI 48913
Helmkerm1@michigan.gov
517-241-3024

2.024 CHANGE REQUESTS

The State reserves the right to request from time to time any changes to the requirements and specifications of the Contract and the work to be performed by the Contractor under the Contract. During the course of ordinary business, it may become necessary for the State to discontinue certain business practices or create Additional Services/Deliverables. At a minimum, to the extent applicable, Contractor shall provide a detailed outline of all work to be done, including tasks necessary to accomplish the Additional Services/Deliverables, timeframes, listing of key personnel assigned, estimated hours for each individual per task, and a complete and detailed cost justification.

If the State requests or directs the Contractor to perform any Services/Deliverables that are outside the scope of the Contractor's responsibilities under the Contract ("New Work"), the Contractor must notify the State promptly before commencing performance of the requested activities it believes are New Work. If the Contractor fails to notify the State before commencing performance of the requested activities, any such activities performed before the Contractor gives notice shall be conclusively considered to be in-scope Services/Deliverables and not New Work.

If the State requests or directs the Contractor to perform any services or provide deliverables that are consistent with and similar to the Services/Deliverables being provided by the Contractor under the Contract, but which the Contractor reasonably and in good faith believes are not included within the Statements of Work, then before performing such Services or providing such Deliverables, the Contractor shall notify the State in writing that it considers the Services or Deliverables to be an Additional Service/Deliverable for which the Contractor should receive additional compensation. If the Contractor does not so notify the State, the Contractor shall have no right to claim thereafter that it is entitled to additional compensation for performing that Service or providing that Deliverable. If the Contractor does so notify the State, then such a Service or Deliverable shall be governed by the Change Request procedure in this Section.

In the event prices or service levels are not acceptable to the State, the Additional Services or New Work shall be subject to competitive bidding based upon the specifications.

- (1) **Change Request at State Request**
If the State requires Contractor to perform New Work, Additional Services or make changes to the Services that would affect the Contract completion schedule or the amount of compensation due Contractor (a "Change"), the State shall submit a written request for Contractor to furnish a proposal for carrying out the requested Change (a "Change Request").
- (2) **Contractor Recommendation for Change Requests:**
Contractor shall be entitled to propose a Change to the State, on its own initiative, should Contractor believe the proposed Change would benefit the Contract.
- (3) Upon receipt of a Change Request or on its own initiative, Contractor shall examine the implications of the requested Change on the technical specifications, Contract schedule and price of the Deliverables and Services and shall submit to the State without undue delay a written proposal for carrying out the Change. Contractor's proposal shall include any associated changes in the technical specifications, Contract schedule and price and method of pricing of the Services. If the Change is to be performed on a time and materials basis, the Amendment Labor Rates shall apply to the provision of such Services. If Contractor provides a written proposal and should Contractor be of the opinion that a requested Change is not to be recommended, it shall communicate its opinion to the State but shall nevertheless carry out the Change as specified in the written proposal if the State directs it to do so.
- (4) By giving Contractor written notice within a reasonable time, the State shall be entitled to accept a Contractor proposal for Change, to reject it, or to reach another agreement with Contractor. Should the parties agree on carrying out a Change, a written Contract Change Notice must be prepared and issued under this Contract, describing the Change and its effects on the Services and any affected components of this Contract (a "Contract Change Notice").
- (5) No proposed Change shall be performed until the proposed Change has been specified in a duly executed Contract Change Notice issued by the Department of Technology, Management & Budget, Procurement.
- (6) If the State requests or directs the Contractor to perform any activities that Contractor believes constitute a Change, the Contractor must notify the State that it believes the requested activities are a Change before beginning to work on the requested activities. If the Contractor fails to notify the State before beginning to work on the requested activities, then the Contractor waives any right to assert any claim for additional compensation or time for performing the requested activities. If the Contractor commences performing work outside the scope of this Contract and then ceases performing that work, the Contractor must, at the request of the State, retract any out-of-scope work that would adversely affect the Contract.

2.025 NOTICES

Any notice given to a party under the Contract must be deemed effective, if addressed to the party as addressed below, upon: (i) delivery, if hand delivered; (ii) receipt of a confirmed transmission by facsimile if a copy of the notice is sent by another means specified in this Section; (iii) the third Business Day after being sent by U.S. mail, postage pre-paid, return receipt requested; or (iv) the next Business Day after being sent by a nationally recognized overnight express courier with a reliable tracking system.

State:

State of Michigan
DTMB-Procurement
Attention:
PO Box 30026
530 West Allegan
Lansing, Michigan 48909

Contractor:

Name:
Address:

Either party may change its address where notices are to be sent by giving notice according to this Section.

2.026 BINDING COMMITMENTS

Representatives of Contractor must have the authority to make binding commitments on Contractor's behalf within the bounds set forth in the Contract. Contractor may change the representatives from time to time upon giving written notice.

2.027 RELATIONSHIP OF THE PARTIES

The relationship between the State and Contractor is that of client and independent contractor. No agent, employee, or servant of Contractor or any of its Subcontractors shall be deemed to be an employee, agent or servant of the State for any reason. Contractor shall be solely and entirely responsible for its acts and the acts of its agents, employees, servants and Subcontractors during the performance of the Contract.

2.028 COVENANT OF GOOD FAITH

Each party shall act reasonably and in good faith. Unless stated otherwise in the Contract, the parties shall not unreasonably delay, condition or withhold the giving of any consent, decision or approval that is either requested or reasonably required of them in order for the other party to perform its responsibilities under the Contract.

2.029 ASSIGNMENTS

Neither party may assign the Contract, or assign or delegate any of its duties or obligations under the Contract, to any other party (whether by operation of law or otherwise), without the prior written consent of the other party; provided, however, that the State may assign the Contract to any other State agency, department, division or department without the prior consent of Contractor and Contractor may assign the Contract to an affiliate so long as the affiliate is adequately capitalized and can provide adequate assurances that the affiliate can perform the Contract. The State may withhold consent from proposed assignments, subcontracts, or novations when the transfer of responsibility would operate to decrease the State's likelihood of receiving performance on the Contract or the State's ability to recover damages.

Contractor may not, without the prior written approval of the State, assign its right to receive payments due under the Contract. If the State permits an assignment, the Contractor is not relieved of its responsibility to perform any of its contractual duties and the requirement under the Contract that all payments must be made to one entity continues.

If the Contractor intends to assign the contract or any of the Contractor's rights or duties under the Contract, the Contractor must notify the State in writing at least 90 days before the assignment. The Contractor also must provide the State with adequate information about the assignee within a reasonable amount of time before the assignment for the State to determine whether to approve the assignment.

2.030 General Provisions

2.031 ADMINISTRATIVE FEE AND REPORTING

The Contractor must remit an administrative fee of 1% on all payments remitted to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales.

Itemized purchasing activity reports should be mailed to DTMB-Procurement and the administrative fee payments shall be made by check payable to the State of Michigan and mailed to:

The Department of Technology, Management & Budget
Updated 8/20/2012

Financial Services – Cashier Unit
Lewis Cass Building
320 South Walnut St.
P.O. Box 30681
Lansing, MI 48909

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each quarter.

2.032 MEDIA RELEASES

News releases (including promotional literature and commercial advertisements) pertaining to the RFP and Contract or project to which it relates shall not be made without prior written State approval, and then only in accordance with the explicit written instructions from the State. No results of the activities associated with the RFP and Contract are to be released without prior written approval of the State and then only to persons designated.

2.033 CONTRACT DISTRIBUTION

DTMB-Procurement retains the sole right of Contract distribution to all State agencies and local units of government unless other arrangements are authorized by DTMB-Procurement.

2.034 PERMITS

Contractor must obtain and pay any associated costs for all required governmental permits, licenses and approvals for the delivery, installation and performance of the Services. The State shall pay for all costs and expenses incurred in obtaining and maintaining any necessary easements or right of way.

2.035 WEBSITE INCORPORATION

The State is not bound by any content on the Contractor's website, even if the Contractor's documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the State has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by an authorized representative of the State.

2.036 FUTURE BIDDING PRECLUSION

Contractor acknowledges that, to the extent this Contract involves the creation, research, investigation or generation of a future RFP, it may be precluded from bidding on the subsequent RFP. The State reserves the right to disqualify any Bidder if the State determines that the Bidder has used its position (whether as an incumbent Contractor, or as a Contractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP.

2.037 FREEDOM OF INFORMATION

All information in any proposal submitted to the State by Contractor and this Contract is subject to the provisions of the Michigan Freedom of Information Act, 1976 Public Act No. 442, as amended, MCL 15.231, et seq (the "FOIA").

2.038 DISASTER RECOVERY

Contractor and the State recognize that the State provides essential services in times of natural or man-made disasters. Therefore, except as so mandated by Federal disaster response requirements, Contractor personnel dedicated to providing Services/Deliverables under this Contract shall provide the State with priority service for repair and work around in the event of a natural or man-made disaster.

2.040 Financial Provisions

2.041 FIXED PRICES FOR SERVICES/DELIVERABLES

Each Statement of Work or Purchase Order issued under this Contract shall specify (or indicate by reference to the appropriate Contract Exhibit) the firm, fixed prices for all Services/Deliverables, and the associated payment milestones and payment amounts. The State may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor shall show verification of measurable progress at the time of requesting progress payments.

2.042 ADJUSTMENTS FOR REDUCTIONS IN SCOPE OF SERVICES/DELIVERABLES

If the scope of the Services/Deliverables under any Statement of Work issued under this Contract is subsequently reduced by the State, the parties shall negotiate an equitable reduction in Contractor's charges under such Statement of Work commensurate with the reduction in scope.

2.043 SERVICES/DELIVERABLES COVERED

The State shall not be obligated to pay any amounts in addition to the charges specified in this Contract for all Services/Deliverables to be provided by Contractor and its Subcontractors, if any, under this Contract,.

2.044 INVOICING AND PAYMENT – IN GENERAL

- (a) Each Statement of Work issued under this Contract shall list (or indicate by reference to the appropriate Contract Exhibit) the prices for all Services/Deliverables, equipment and commodities to be provided, and the associated payment milestones and payment amounts.
 - (b) Each Contractor invoice shall show details as to charges by Service/Deliverable component and location at a level of detail reasonably necessary to satisfy the State's accounting and charge-back requirements. Invoices for Services performed on a time and materials basis shall show, for each individual, the number of hours of Services performed during the billing period, the billable skill/labor category for such person and the applicable hourly billing rate. Prompt payment by the State is contingent on the Contractor's invoices showing the amount owed by the State minus any holdback amount to be retained by the State in accordance with **Section 1.600**.
 - (c) Correct invoices shall be due and payable by the State, in accordance with the State's standard payment procedure as specified in 1984 Public Act No. 279, MCL 17.51 et seq., within 45 days after receipt, provided the State determines that the invoice was properly rendered.
- (d1) All invoices should reflect actual work done. Specific details of invoices and payments shall be agreed upon between the Contract Administrator and the Contractor after the proposed Contract Agreement has been signed and accepted by both the Contractor and the Director of Procurement, Department of Management & Budget. This activity shall occur only upon the specific written direction from DTMB-Procurement.

The specific payment schedule for any Contract(s) entered into, as the State and the Contractor(s) shall mutually agree upon. The schedule should show payment amount and should reflect actual work done by the payment dates, less any penalty cost charges accrued by those dates. As a general policy statements shall be forwarded to the designated representative by the 15th day of the following month.

The Government may make progress payments to the Contractor when requested as work progresses, but not more frequently than monthly, in amounts approved by the Contract Administrator, after negotiation. Contractor must show verification of measurable progress at the time of requesting progress payments.

- (d2) Contract Payment Schedule
 - 1. Contractor request for performance-based payment.

The Contractor may submit requests for payment of performance-based payments not more frequently than monthly, in a form and manner acceptable to the Contract Administrator. Unless otherwise authorized by the Contract Administrator, all performance-based payments in any period for which payment is being requested shall be included in a single request, appropriately itemized and totaled.

2. Approval and payment of requests.

The Contractor shall not be entitled to payment of a request for performance-based payment prior to successful accomplishment of the event or performance criterion for which payment is requested. The Contract Administrator shall determine whether the event or performance criterion for which payment is requested has been successfully accomplished in accordance with the terms of the contract. The Contract Administrator may, at any time, require the Contractor to substantiate the successful performance of any event or performance criterion, which has been or is represented as being payable.

A payment under this performance-based payment clause is a contract financing payment under the Quick Payment Terms in **Section 1.600** of this Contract.

The approval by the Contract Administrator of a request for performance-based payment does not constitute an acceptance by the Government and does not excuse the Contractor from performance of obligations under this Contract.

2.045 PRO-RATION

To the extent there are Services that are to be paid for on a monthly basis, the cost of such Services shall be pro-rated for any partial month.

2.046 ANTITRUST ASSIGNMENT

The Contractor assigns to the State any claim for overcharges resulting from antitrust violations to the extent that those violations concern materials or services supplied by third parties to the Contractor, toward fulfillment of this Contract.

2.047 FINAL PAYMENT

The making of final payment by the State to Contractor does not constitute a waiver by either party of any rights or other claims as to the other party's continuing obligations under the Contract, nor shall it constitute a waiver of any claims by one party against the other arising from unsettled claims or failure by a party to comply with this Contract, including claims for Services and Deliverables not reasonably known until after acceptance to be defective or substandard. Contractor's acceptance of final payment by the State under this Contract shall constitute a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still unsettled.

2.048 ELECTRONIC PAYMENT REQUIREMENT

Electronic transfer of funds is required for payments on State Contracts. Contractors are required to register with the State electronically at <http://www.cpexpress.state.mi.us>. As stated in Public Act 431 of 1984, all contracts that the State enters into for the purchase of goods and services shall provide that payment shall be made by electronic fund transfer (EFT).

2.050 Taxes

2.051 EMPLOYMENT TAXES

Contractor shall collect and pay all applicable federal, state, and local employment taxes, including the taxes.

2.052 SALES AND USE TAXES

Contractor shall register and remit sales and use taxes on taxable sales of tangible personal property or services delivered into the State. Contractors that lack sufficient presence in Michigan to be required to register and pay tax must do so as a volunteer. This requirement extends to: (1) all members of any controlled group as defined in § 1563(a) of the Internal Revenue Code and applicable regulations of which the company is a member, and (2) all organizations under common control as defined in § 414(c) of the Internal Revenue Code and applicable regulations of which the company is a member that make sales at retail for delivery into the State are registered with the State for the collection and remittance of sales and use taxes. In applying treasury regulations defining “two or more trades or businesses under common control” the term “organization” means sole proprietorship, a partnership (as defined in § 701(a)(2) of the Internal Revenue Code), a trust, an estate, a corporation, or a limited liability company.

2.060 Contract Management

2.061 CONTRACTOR PERSONNEL QUALIFICATIONS

All persons assigned by Contractor to the performance of Services under this Contract must be employees of Contractor or its majority-owned (directly or indirectly, at any tier) subsidiaries (or a State-approved Subcontractor) and must be fully qualified to perform the work assigned to them. Contractor must include a similar provision in any subcontract entered into with a Subcontractor. For the purposes of this Contract, independent contractors engaged by Contractor solely in a staff augmentation role must be treated by the State as if they were employees of Contractor for this Contract only; however, the State understands that the relationship between Contractor and Subcontractor is an independent contractor relationship.

2.062 CONTRACTOR KEY PERSONNEL

- (a) The Contractor must provide the Contract Compliance Inspector with the names of the Key Personnel.
- (b) Key Personnel must be dedicated as defined in the Statement of Work to the Project for its duration in the applicable Statement of Work with respect to other individuals designated as Key Personnel for that Statement of Work.
- (c) The State shall have the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor shall notify the State of the proposed assignment, shall introduce the individual to the appropriate State representatives, and shall provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State shall provide a written explanation including reasonable detail outlining the reasons for the rejection.
- (d) Contractor must not remove any Key Personnel from their assigned roles on the Contract without the prior written consent of the State. The Contractor’s removal of Key Personnel without the prior written consent of the State is an unauthorized removal (“Unauthorized Removal”). Unauthorized Removals does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation or for cause termination of the Key Personnel’s employment. Unauthorized Removals does not include replacing Key Personnel because of promotions or other job movements allowed by Contractor personnel policies or Collective Bargaining Agreement(s) as long as the State receives prior written notice before shadowing occurs and Contractor provides 30 days of shadowing unless parties agree to a different time period. The Contractor with the State must review any Key Personnel replacements, and appropriate transition planning will be established. Any Unauthorized Removal may be considered by the State to be a material breach of the Contract, in respect of which the State may elect to exercise its termination and cancellation rights.
- (e) The Contractor must notify the Contract Compliance Inspector and the Contract Administrator at least 10 business days before redeploying non-Key Personnel, who are dedicated to primarily to the

Project, to other projects. If the State does not object to the redeployment by its scheduled date, the Contractor may then redeploy the non-Key Personnel.

2.063 RE-ASSIGNMENT OF PERSONNEL AT THE STATE'S REQUEST

The State reserves the right to require the removal from the Project of Contractor personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request must be based on legitimate, good faith reasons. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed personnel, the State agrees to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any incident with removed personnel results in delay not reasonably anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Service shall not be counted for a time as agreed to by the parties.

2.064 CONTRACTOR PERSONNEL LOCATION

All staff assigned by Contractor to work on the Contract shall perform their duties either primarily at Contractor's offices and facilities or at State facilities. Without limiting the generality of the foregoing, Key Personnel shall, at a minimum, spend at least the amount of time on-site at State facilities as indicated in the applicable Statement of Work. Subject to availability, selected Contractor personnel may be assigned office space to be shared with State personnel.

2.065 CONTRACTOR IDENTIFICATION

Contractor employees must be clearly identifiable while on State property by wearing a State-issued badge, as required. Contractor employees are required to clearly identify themselves and the company they work for whenever making contact with State personnel by telephone or other means.

2.066 COOPERATION WITH THIRD PARTIES

Contractor agrees to cause its personnel and the personnel of any Subcontractors to cooperate with the State and its agents and other contractors including the State's Quality Assurance personnel. As reasonably requested by the State in writing, the Contractor shall provide to the State's agents and other contractors reasonable access to Contractor's Project personnel, systems and facilities to the extent the access relates to activities specifically associated with this Contract and shall not interfere or jeopardize the safety or operation of the systems or facilities. The State acknowledges that Contractor's time schedule for the Contract is very specific and agrees not to unnecessarily or unreasonably interfere with, delay or otherwise impeded Contractor's performance under this Contract with the requests for access.

2.067 CONTRACT MANAGEMENT RESPONSIBILITIES

Contractor shall be responsible for all acts and omissions of its employees, as well as the acts and omissions of any other personnel furnished by Contractor to perform the Services. Contractor shall have overall responsibility for managing and successfully performing and completing the Services/Deliverables, subject to the overall direction and supervision of the State and with the participation and support of the State as specified in this Contract. Contractor's duties shall include monitoring and reporting the State's performance of its participation and support responsibilities (as well as Contractor's own responsibilities) and providing timely notice to the State in Contractor's reasonable opinion if the State's failure to perform its responsibilities in accordance with the Project Plan is likely to delay the timely achievement of any Contract tasks.

The Contractor shall provide the Services/Deliverables directly or through its affiliates, subsidiaries, subcontractors or resellers. Regardless of the entity providing the Service/Deliverable, the Contractor shall act as a single point of contact coordinating these entities to meet the State's need for Services/Deliverables. Nothing in this Contract, however, shall be construed to authorize or require any party to violate any applicable law or regulation in its performance of this Contract.

2.068 CONTRACTOR RETURN OF STATE EQUIPMENT/RESOURCES

The Contractor shall return to the State any State-furnished equipment, facilities and other resources when no longer required for the Contract in the same condition as when provided by the State, reasonable wear and tear excepted.

2.070 Subcontracting by Contractor

2.071 CONTRACTOR FULL RESPONSIBILITY

Contractor shall have full responsibility for the successful performance and completion of all of the Services and Deliverables. The State shall consider Contractor to be the sole point of contact with regard to all contractual matters under this Contract, including payment of any and all charges for Services and Deliverables.

2.072 STATE CONSENT TO DELEGATION

Contractor shall not delegate any duties under this Contract to a Subcontractor unless the Department of Technology, Management & Budget, Procurement has given written consent to such delegation. The State shall have the right of prior written approval of all Subcontractors and to require Contractor to replace any Subcontractors found, in the reasonable judgment of the State, to be unacceptable. The State's request shall be written with reasonable detail outlining the reasons for the removal request. Additionally, the State's request shall be based on legitimate, good faith reasons. Replacement Subcontractor(s) for the removed Subcontractor shall be fully qualified for the position. If the State exercises this right, and the Contractor cannot immediately replace the removed Subcontractor, the State shall agree to an equitable adjustment in schedule or other terms that may be affected by the State's required removal. If any such incident with a removed Subcontractor results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLA for the affected Work shall not be counted for a time agreed upon by the parties.

2.073 SUBCONTRACTOR BOUND TO CONTRACT

In any subcontracts entered into by Contractor for the performance of the Services, Contractor shall require the Subcontractor, to the extent of the Services to be performed by the Subcontractor, to be bound to Contractor by the terms of this Contract and to assume toward Contractor all of the obligations and responsibilities that Contractor, by this Contract, assumes toward the State. The State reserves the right to receive copies of and review all subcontracts, although Contractor may delete or mask any proprietary information, including pricing, contained in such contracts before providing them to the State. The management of any Subcontractor shall be the responsibility of Contractor, and Contractor shall remain responsible for the performance of its Subcontractors to the same extent as if Contractor had not subcontracted such performance. Contractor shall make all payments to Subcontractors or suppliers of Contractor. Except as otherwise agreed in writing by the State and Contractor, the State shall not be obligated to direct payments for the Services other than to Contractor. The State's written approval of any Subcontractor engaged by Contractor to perform any obligation under this Contract shall not relieve Contractor of any obligations or performance required under this Contract. A list of the Subcontractors, if any, approved by the State as of the execution of this Contract, together with a copy of the applicable subcontract is attached.

2.074 FLOW DOWN

Except where specifically approved in writing by the State on a case-by-case basis, Contractor shall flow down the obligations in **Sections 2.031, 2.060, 2.100, 2.110, 2.120, 2.130, and 2.200** in all of its agreements with any Subcontractors.

2.075 COMPETITIVE SELECTION

The Contractor shall select subcontractors (including suppliers) on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the Contract.

2.080 State Responsibilities

2.081 EQUIPMENT

The State shall provide only the equipment and resources identified in the Statement of Work and other Contract Exhibits.

2.082 FACILITIES

The State must designate space as long as it is available and as provided in the Statement of Work, to house the Contractor's personnel whom the parties agree will perform the Services/Deliverables at State facilities (collectively, the "State Facilities"). The Contractor shall have reasonable access to, and unless agreed otherwise by the parties in writing must observe and comply with all rules and regulations relating to each of the State Facilities (including hours of operation) used by the Contractor in the course of providing the Services. Contractor agrees that it shall not, without the prior written consent of the State, use any State Facilities or access any State information systems provided for the Contractor's use, or to which the Contractor otherwise gains access in the course of performing the Services, for any purpose other than providing the Services to the State.

2.090 Security

2.091 BACKGROUND CHECKS

On a case-by-case basis, the State may investigate the Contractor's personnel before they may have access to State facilities and systems. The scope of the background check is at the discretion of the State and the results shall be used to determine Contractor personnel eligibility for working within State facilities and systems. The investigations shall include Michigan State Police Background checks (ICHAT) and may include the National Crime Information Center (NCIC) Finger Prints. Proposed Contractor personnel may be required to complete and submit an RI-8 Fingerprint Card for the NCIC Finger Print Check. Any request for background checks shall be initiated by the State and shall be reasonably related to the type of work requested.

2.100 Confidentiality

2.101 CONFIDENTIALITY

Contractor and the State each acknowledge that the other possesses and shall continue to possess confidential information that has been developed or received by it. As used in this Section, "Confidential Information" of Contractor must mean all non-public proprietary information of Contractor (other than Confidential Information of the State as defined below), which is marked confidential, restricted, proprietary, or with a similar designation. "Confidential Information" of the State must mean any information which is retained in confidence by the State (or otherwise required to be held in confidence by the State under applicable federal, state and local laws and regulations) or which, in the case of tangible materials provided to Contractor by the State under its performance under this Contract, is marked as confidential, proprietary or with a similar designation by the State. "Confidential Information" excludes any information (including this Contract) that is publicly available under the Michigan FOIA.

2.102 PROTECTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION

The State and Contractor shall each use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication or dissemination of its own confidential information of like character, but in no event less than reasonable care. Neither Contractor nor the State shall (i) make any use of the Confidential Information of the other except as contemplated by this Contract, (ii) acquire any right in or assert any lien against the

Confidential Information of the other, or (iii) if requested to do so, refuse for any reason to promptly return the other party's Confidential Information to the other party. Each party shall limit disclosure of the other party's Confidential Information to employees and Subcontractors who must have access to fulfill the purposes of this Contract. Disclosure to, and use by, a Subcontractor is permissible where (A) use of a Subcontractor is authorized under this Contract, (B) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Subcontractor's scope of responsibility, and (C) Contractor obligates the Subcontractor in a written Contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor and of any Subcontractor having access or continued access to the State's Confidential Information may be required to execute an acknowledgment that the employee has been advised of Contractor's and the Subcontractor's obligations under this Section and of the employee's obligation to Contractor or Subcontractor, as the case may be, to protect the Confidential Information from unauthorized use or disclosure.

Promptly upon termination or cancellation of the Contract for any reason, Contractor must certify to the State that Contractor has destroyed all State Confidential Information.

2.103 PCI DATA SECURITY STANDARD

(a) Contractors that process, transmit or store credit/debit cardholder data, must adhere to the Payment Card Industry (PCI) Data Security Standards. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

(b) The Contractor must notify the CCI (within 72 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the Visa, MasterCard, Discover and state Acquirer representative(s), and/or a PCI approved third party to conduct a thorough security review. The Contractor must make the forensic report available within two weeks of completion. The review must validate compliance with the current PCI Data Security Standards for protecting cardholder data.

(c) The Contractor must properly dispose of cardholder data, in compliance with DTMB policy, when it is no longer needed. The Contractor must continue to treat cardholder data as confidential upon contract termination.

(d) The Contractor must provide the CCI with an annual Attestation of Compliance (AOC) or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standards. The Contractor must notify the CCI of all failures to comply with the PCI Data Security Standard.

2.104 EXCLUSIONS

Notwithstanding the foregoing, the provisions in this Section shall not apply to any particular information which the State or Contractor can demonstrate (i) was, at the time of disclosure to it, in the public domain; (ii) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party; (iii) was in the possession of the receiving party at the time of disclosure to it without an obligation of confidentiality; (iv) was received after disclosure to it from a third party who had a lawful right to disclose the information to it without any obligation to restrict its further disclosure; or (v) was independently developed by the receiving party without reference to Confidential Information of the furnishing party. Further, the provisions of this Section shall not apply to any particular Confidential Information to the extent the receiving party is required by law to disclose the Confidential Information, provided that the receiving party (i) promptly provides the furnishing party with notice of the legal request, and (ii) assists the furnishing party in resisting or limiting the scope of the disclosure as reasonably requested by the furnishing party.

2.105 NO IMPLIED RIGHTS

Nothing contained in this Section must be construed as obligating a party to disclose any particular Confidential Information to the other party, or as granting to or conferring on a party, expressly or impliedly, any right or license to the Confidential Information of the other party.

2.106 SECURITY BREACH NOTIFICATION

If the Contractor breaches this Section, the Contractor must (i) promptly cure any deficiencies and (ii) comply with any applicable federal and state laws and regulations pertaining to unauthorized disclosures. Contractor and the State shall cooperate to mitigate, to the extent practicable, the effects of any breach, intrusion, or unauthorized use or disclosure. Contractor must report to the State in writing any use or disclosure of Confidential Information, whether suspected or actual, other than as provided for by the Contract within 72 hours of becoming aware of the use or disclosure or the shorter time period as is reasonable under the circumstances.

2.107 RESPECTIVE OBLIGATIONS

The parties' respective obligations under this Section must survive the termination or expiration of this Contract for any reason.

2.110 Records and Inspections

2.111 INSPECTION OF WORK PERFORMED

The State's authorized representatives, at reasonable times and with 10 days prior notice, have the right to enter the Contractor's premises or any other places where work is being performed in relation to this Contract. The representatives may inspect, monitor, or evaluate the work being performed, to the extent the access will not reasonably interfere with or jeopardize the safety or operation of Contractor's systems or facilities. The Contractor must provide reasonable assistance for the State's representatives during inspections.

2.112 RETENTION OF RECORDS

(a) The Contractor must retain all financial and accounting records related to this Contract for a period of 7 years after the Contractor performs any work under this Contract (Audit Period).

(b) If an audit, litigation, or other action involving the Contractor's records is initiated before the end of the Audit Period, the Contractor must retain the records until all issues arising out of the audit, litigation, or other action are resolved or until the end of the Audit Period, whichever is later.

2.113 EXAMINATION OF RECORDS

(a) The State, upon 10 days notice to the Contractor, may examine and copy any of the Contractor's records that relate to this Contract any time during the Audit Period. The State does not have the right to review any information deemed confidential by the Contractor if access would require the information to become publicly available. This requirement also applies to the records of any parent, affiliate, or subsidiary organization of the Contractor, or any Subcontractor that performs services in connection with this Contract

(b) In addition to the rights conferred upon the State in paragraph (a) of this section and in accordance with MCL 18.1470, DTMB or its designee may audit the Contractor to verify compliance with the Contract. The financial and accounting records associated with the Contract shall be made available to DTMB or its designee and the auditor general, upon request, during the term of the Contract and any extension of the Contract and for 3 years after the later of the expiration date or final payment under the Contract.

2.114 AUDIT RESOLUTION

If necessary, the Contractor and the State will meet to review any audit report promptly after its issuance. The Contractor must respond to each report in writing within 30 days after receiving the report, unless the report specifies a shorter response time. The Contractor and the State must develop, agree upon, and monitor an action plan to promptly address and resolve any deficiencies, concerns, or recommendations in the report.

2.115 ERRORS

(a) If an audit reveals any financial errors in the records provided to the State, the amount in error must be reflected as a credit or debit on the next invoice and subsequent invoices until the amount is paid or refunded in full. However, a credit or debit may not be carried forward for more than four invoices or beyond the termination of the Contract. If a balance remains after four invoices, the remaining amount will be due as a payment or refund within 45 days of the last invoice on which the balance appeared or upon termination of the Contract, whichever is earlier.

(b) In addition to other available remedies, if the difference between the State's actual payment and the correct invoice amount, as determined by an audit, is greater than 10%, the Contractor must pay all reasonable audit costs.

2.120 Warranties

2.121 WARRANTIES AND REPRESENTATIONS

The Contractor represents and warrants:

- (a) It is capable in all respects of fulfilling and must fulfill all of its obligations under this Contract. The performance of all obligations under this Contract must be provided in a timely, professional, and workman-like manner and must meet the performance and operational standards required under this Contract.
- (b) The Contract Appendices, Attachments and Exhibits identify the equipment and software and services necessary for the Deliverable(s) to perform and Services to operate in compliance with the Contract's requirements and other standards of performance.
- (c) It is the lawful owner or licensee of any Deliverable licensed or sold to the State by Contractor or developed by Contractor under this Contract, and Contractor has all of the rights necessary to convey to the State the ownership rights or licensed use, as applicable, of any and all Deliverables. None of the Deliverables provided by Contractor to the State under neither this Contract, nor their use by the State shall infringe the patent, copyright, trade secret, or other proprietary rights of any third party.
- (d) If, under this Contract, Contractor procures any equipment, software or other Deliverable for the State (including equipment, software and other Deliverables manufactured, re-marketed or otherwise sold by Contractor under Contractor's name), then in addition to Contractor's other responsibilities with respect to the items in this Contract, Contractor must assign or otherwise transfer to the State or its designees, or afford the State the benefits of, any manufacturer's warranty for the Deliverable.
- (e) The contract signatory has the power and authority, including any necessary corporate authorizations, necessary to enter into this Contract, on behalf of Contractor.
- (f) It is qualified and registered to transact business in all locations where required.
- (g) Neither the Contractor nor any Affiliates, nor any employee of either, has, must have, or must acquire, any contractual, financial, business, or other interest, direct or indirect, that would conflict in any manner or degree with Contractor's performance of its duties and responsibilities to the State under this Contract or otherwise create an appearance of impropriety with respect to the award or performance of this Agreement. Contractor must notify the State about the nature of the conflict or appearance of impropriety within two days of learning about it.
- (h) Neither Contractor nor any Affiliates, nor any employee of either has accepted or must accept anything of value based on an understanding that the actions of the Contractor or Affiliates or

employee on behalf of the State would be influenced. Contractor must not attempt to influence any State employee by the direct or indirect offer of anything of value.

- (i) Neither Contractor nor any Affiliates, nor any employee of either has paid or agreed to pay any person, other than bona fide employees and consultants working solely for Contractor or the Affiliate, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Contract.
- (j) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Bidder; and no attempt was made by Contractor to induce any other person to submit or not submit a proposal for the purpose of restricting competition.
- (k) All financial statements, reports, and other information furnished by Contractor to the State as part of its response to the RFP or otherwise in connection with the award of this Contract fairly and accurately represent the business, properties, financial condition, and results of operations of Contractor as of the respective dates, or for the respective periods, covered by the financial statements, reports, other information. Since the respective dates or periods covered by the financial statements, reports, or other information, there have been no material adverse changes in the business, properties, financial condition, or results of operations of Contractor.
- (l) All written information furnished to the State by or for the Contractor in connection with this Contract, including its bid, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading.
- (m) It is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State or the department within the previous five years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract.
- (n) If any of the certifications, representations, or disclosures made in the Contractor's original bid response change after contract award, the Contractor is required to report those changes immediately to the Department of Technology, Management & Budget, Procurement.

2.122 WARRANTY OF MERCHANTABILITY

Goods provided by Contractor under this agreement shall be merchantable. All goods provided under this Contract shall be of good quality within the description given by the State, shall be fit for their ordinary purpose, shall be adequately contained and packaged within the description given by the State, shall conform to the agreed upon specifications, and shall conform to the affirmations of fact made by the Contractor or on the container or label.

2.123 WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE

When the Contractor has reason to know or knows any particular purpose for which the goods are required, and the State is relying on the Contractor's skill or judgment to select or furnish suitable goods, there is a warranty that the goods are fit for such purpose.

2.124 WARRANTY OF TITLE

Contractor shall, in providing goods to the State, convey good title in those goods, whose transfer is right and lawful. All goods provided by Contractor shall be delivered free from any security interest, lien, or encumbrance of which the State, at the time of contracting, has no knowledge. Goods provided by Contractor, under this Contract, shall be delivered free of any rightful claim of any third person by of infringement or the like.

2.125 EQUIPMENT WARRANTY

To the extent Contractor is responsible under this Contract for maintaining equipment/system(s), Contractor represents and warrants that it shall maintain the equipment/system(s) in good operating condition and shall undertake all repairs and preventive maintenance according to the applicable manufacturer's recommendations for the period specified in this Contract.

The Contractor represents and warrants that the equipment/system(s) are in good operating condition and operates and performs to the requirements and other standards of performance contained in this Contract, when installed, at the time of Final Acceptance by the State, and for a period of (1) one year commencing upon the first day following Final Acceptance.

Within 60 business days of notification from the State, the Contractor must adjust, repair or replace all equipment that is defective or not performing in compliance with the Contract. The Contractor must assume all costs for replacing parts or units and their installation including transportation and delivery fees, if any.

The Contractor must provide a toll-free telephone number to allow the State to report equipment failures and problems to be remedied by the Contractor.

The Contractor agrees that all warranty service it provides under this Contract must be performed by Original Equipment Manufacturer (OEM) trained, certified and authorized technicians.

The Contractor is the sole point of contact for warranty service. The Contractor warrants that it shall pass through to the State any warranties obtained or available from the original equipment manufacturer, including any replacement, upgraded, or additional equipment warranties.

2.126 EQUIPMENT TO BE NEW

If applicable, all equipment provided under this Contract by Contractor shall be new where Contractor has knowledge regarding whether the equipment is new or assembled from new or serviceable used parts that are like new in performance or has the option of selecting one or the other. Equipment that is assembled from new or serviceable used parts that are like new in performance is acceptable where Contractor does not have knowledge or the ability to select one or other, unless specifically agreed otherwise in writing by the State.

2.127 PROHIBITED PRODUCTS

The State will not accept salvage, distressed, outdated or discontinued merchandise. Shipping of such merchandise to any State agency, as a result of an order placed against the Contract, shall be considered default by the Contractor of the terms and conditions of the Contract and may result in cancellation of the Contract by the State. The brand and product number offered for all items shall remain consistent for the term of the Contract, unless DTMB-Procurement has approved a change order pursuant to **Section 2.024**.

2.128 CONSEQUENCES FOR BREACH

In addition to any remedies available in law, if the Contractor breaches any of the warranties contained in this section, the breach may be considered as a default in the performance of a material obligation of this Contract.

2.130 Insurance

2.13.1 LIABILITY INSURANCE

For the purpose of this Section, "State" includes its departments, divisions, agencies, offices, commissions, officers, employees, and agents.

(a) The Contractor must provide proof that it has obtained the minimum levels of insurance coverage indicated or required by law, whichever is greater. The insurance must protect the State from claims that may arise out of, or result from, or are alleged to arise out of, or result from, the Contractor's or a Subcontractor's performance, including any person directly or indirectly employed by the Contractor or a Subcontractor, or any person for whose acts the Contractor or a Subcontractor may be liable.

(b) The Contractor waives all rights against the State for the recovery of damages that are covered by the insurance policies the Contractor is required to maintain under this Section. The Contractor's failure to obtain and maintain the required insurance will not limit this waiver.

(c) All insurance coverage provided relative to this Contract is primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State.

(d) The State, in its sole discretion, may approve the use of a fully-funded self-insurance program in place of any specified insurance identified in this Section.

(e) Unless the State approves otherwise, any insurer must have an A.M. Best rating of "A" or better and a financial size of VII or better, or if those ratings are not available, a comparable rating from an insurance rating agency approved by the State. All policies of insurance must be issued by companies that have been approved to do business in the State.

(f) Where specific coverage limits are listed in this Section, they represent the minimum acceptable limits. If the Contractor's policy contains higher limits, the State is entitled to coverage to the extent of the higher limits.

(g) The Contractor must maintain all required insurance coverage throughout the term of this Contract and any extensions. However, in the case of claims-made Commercial General Liability policies, the Contractor must secure tail coverage for at least three (3) years following the termination of this Contract.

(h) The Contractor must provide, within five (5) business days, written notice to the Director of DTMB-Procurement if any policy required under this section is cancelled. The notice must include the applicable Contract or Purchase Order number.

(i) The minimum limits of coverage specified are not intended, and may not be construed, to limit any liability or indemnity of the Contractor to any indemnified party or other persons.

(j) The Contractor is responsible for the payment of all deductibles.

(k) If the Contractor fails to pay any premium for a required insurance policy, or if any insurer cancels or significantly reduces any required insurance without the State's approval, the State may, after giving the Contractor at least 30 days' notice, pay the premium or procure similar insurance coverage from another company or companies. The State may deduct any part of the cost from any payment due the Contractor, or require the Contractor to pay that cost upon demand.

(l) In the event the State approves the representation of the State by the insurer's attorney, the attorney may be required to be designated as a Special Assistant Attorney General by the Michigan Attorney General.

(m) The Contractor is required to pay for and provide the type and amount of insurance checked below:

(i) Commercial General Liability

Minimal Limits:

\$2,000,000 General Aggregate Limit other than Products/Completed Operations

\$2,000,000 Products/Completed Operations Aggregate Limit

\$1,000,000 Personal & Advertising Injury Limit, and

\$1,000,000 Each Occurrence Limit.

Deductible maximum:

\$50,000 Each Occurrence

Additional Requirements:

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the Commercial General Liability certificate. The Contractor also agrees to provide evidence that the insurance policy contains a waiver of subrogation by the insurance company.

The Products/Completed Operations sublimit requirement may be satisfied by evidence of the manufacturer's Commercial General Liability Insurance. The manufacturer must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the Commercial General Liability certificate and must provide evidence that the policy contains a waiver of subrogation by the insurance company.

(ii) Motor Vehicle

Minimal Limits:

If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.

(iii) Workers' Compensation

Minimal Limits:

The Contractor must provide Workers' Compensation coverage according to applicable laws governing work activities in the state of the Contractor's domicile. If the applicable coverage is provided by a self-insurer, the Contractor must provide proof of an approved self-insured authority by the jurisdiction of domicile.

For employees working outside of the state of the Contractor's domicile, the Contractor must provide certificates of insurance proving mandated coverage levels for the jurisdictions where the employees' activities occur.

Additional Requirements:

The Contractor must provide the applicable certificates of insurance and a list of states where the coverage is applicable. Contractor must provide proof that the Workers' Compensation insurance policies contain a waiver of subrogation by the insurance company, except where such a provision is prohibited or limited by the laws of the jurisdiction in which the work is to be performed.

(iv) Employers Liability

Minimal Limits:

\$100,000 Each Incident
\$100,000 Each Employee by Disease
\$500,000 Aggregate Disease

Additional Requirements:

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the certificate.

(v) Professional Liability (Errors and Omissions)

Minimal Limits:

\$3,000,000 Each Occurrence
\$3,000,000 Annual Aggregate

Deductible Maximum:

\$50,000 Per Loss

(ix) Cyber Liability

Minimal Limits:

\$1,000,000 Each Occurrence
\$1,000,000 Annual Aggregate

Additional Requirements:

Insurance should cover (a) unauthorized acquisition, access, use, physical taking, identity theft, mysterious disappearance, release, distribution or disclosures of personal and corporate information; (b) Transmitting or receiving malicious code via the insured's computer system; (c) Denial of service attacks or the inability to access websites or computer systems.

The Contractor must list the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents as additional insureds on the certificate.

2.13.2 SUBCONTRACTOR INSURANCE COVERAGE

Except where the State has approved a subcontract with other insurance provisions, the Contractor must require any Subcontractor to purchase and maintain the insurance coverage required in Section 2.13.1, Liability Insurance. Alternatively, the Contractor may include a Subcontractor under the Contractor's insurance on the coverage required in that Section. The failure of a Subcontractor to comply with insurance requirements does not limit the Contractor's liability or responsibility.

2.13.3 CERTIFICATES OF INSURANCE

Before the Contract is signed, and not less than 20 days before the insurance expiration date every year thereafter, the Contractor must provide evidence that the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents are listed as additional insureds as required. The Contractor must provide DTMB-Procurement with all applicable certificates of insurance verifying insurance coverage or providing, if approved, satisfactory evidence of self-insurance as required in Section 2.13.1, Liability Insurance. Each certificate must be on the standard "Accord" form or equivalent and MUST IDENTIFY THE APPLICABLE CONTRACT OR PURCHASE ORDER NUMBER.

2.140 Indemnification

2.141 GENERAL INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from liability, including all claims and losses, and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties), accruing or resulting to any person, firm or corporation that may be injured or damaged by the Contractor in the performance of this Contract and that are attributable to the negligence or tortious acts of the Contractor or any of its subcontractors, or by anyone else for whose acts any of them may be liable.

2.142 CODE INDEMNIFICATION

To the extent permitted by law, the Contractor shall indemnify, defend and hold harmless the State from any claim, loss, or expense arising from Contractor's breach of the No Surreptitious Code Warranty.

2.143 EMPLOYEE INDEMNIFICATION

In any claims against the State of Michigan, its departments, divisions, agencies, sections, commissions, officers, employees and agents, by any employee of the Contractor or any of its subcontractors, the indemnification obligation under the Contract must not be limited in any way by the amount or type of damages, compensation or benefits payable by or for the Contractor or any of its subcontractors under worker's disability compensation acts, disability benefit acts or other employee benefit acts. This indemnification clause is intended to be comprehensive. Any overlap in provisions, or the fact that greater specificity is provided as to some categories of risk, is not intended to limit the scope of indemnification under any other provisions.

2.144 PATENT/COPYRIGHT INFRINGEMENT INDEMNIFICATION

To the extent permitted by law, the Contractor must indemnify, defend and hold harmless the State from and against all losses, liabilities, damages (including taxes), and all related costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) incurred in connection with any action or proceeding threatened or brought against the State to the extent that the action or proceeding is based on a claim that any piece of equipment, software, commodity or service supplied by the Contractor or its subcontractors, or the operation of the equipment, software, commodity or service, or the use or reproduction of any documentation provided with the equipment, software, commodity or service infringes any United States patent, copyright, trademark or trade secret of any person or entity, which is enforceable under the laws of the United States.

In addition, should the equipment, software, commodity, or service, or its operation, become or in the State's or Contractor's opinion be likely to become the subject of a claim of infringement, the Contractor must at the Contractor's sole expense (i) procure for the State the right to continue using the equipment, software, commodity or service or, if the option is not reasonably available to the Contractor, (ii) replace or modify to the State's satisfaction the same with equipment, software, commodity or service of equivalent function and performance so that it becomes non-infringing, or, if the option is not reasonably available to Contractor, (iii) accept its return by the State with appropriate credits to the State against the Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

Notwithstanding the foregoing, the Contractor has no obligation to indemnify or defend the State for, or to pay any costs, damages or attorneys' fees related to, any claim based upon (i) equipment developed based on written specifications of the State; (ii) use of the equipment in a configuration other than implemented or approved in writing by the Contractor, including, but not limited to, any modification of the equipment by the State; or (iii) the combination, operation, or use of the equipment with equipment or software not supplied by the Contractor under this Contract.

2.145 CONTINUATION OF INDEMNIFICATION OBLIGATIONS

The Contractor's duty to indemnify under this Section continues in full force and effect, notwithstanding the expiration or early cancellation of the Contract, with respect to any claims based on facts or conditions that occurred before expiration or cancellation.

2.146 INDEMNIFICATION PROCEDURES

The procedures set forth below must apply to all indemnity obligations under this Contract.

- (a) After the State receives notice of the action or proceeding involving a claim for which it shall seek indemnification, the State must promptly notify Contractor of the claim in writing and take or assist Contractor in taking, as the case may be, any reasonable action to avoid the imposition of a default judgment against Contractor. No failure to notify the Contractor relieves the Contractor of its indemnification obligations except to the extent that the Contractor can prove damages attributable to the failure. Within 10 days following receipt of written notice from the State relating to any claim, the Contractor must notify the State in writing whether Contractor agrees to assume control of the defense and settlement of that claim (a "Notice of Election"). After notifying Contractor of a claim and before the State receiving Contractor's Notice of Election, the State is entitled to defend against the claim, at the Contractor's expense, and the Contractor will be responsible for any reasonable costs incurred by the State in defending against the claim during that period.
- (b) If Contractor delivers a Notice of Election relating to any claim: (i) the State is entitled to participate in the defense of the claim and to employ counsel at its own expense to assist in the handling of the claim and to monitor and advise the State about the status and progress of the defense; (ii) the Contractor must, at the request of the State, demonstrate to the reasonable satisfaction of the State, the Contractor's financial ability to carry out its defense and indemnity obligations under this Contract; (iii) the Contractor must periodically advise the State about the status and progress of the defense and must obtain the prior written approval of the State before entering into any settlement of the claim or ceasing to defend against the claim; and (iv) to the extent that any principles of Michigan governmental or public law may be involved or challenged, the State has the right, at its own expense, to control the defense of that portion of the claim involving the principles of Michigan governmental or public law. But the State may retain control of the defense and settlement of a claim by notifying the Contractor in writing within 10 days after the State's receipt of Contractor's information requested by the State under clause (ii) of this paragraph if the State determines that the Contractor has failed to demonstrate to the reasonable satisfaction of the State the Contractor's financial ability to carry out its defense and indemnity obligations under this Section. Any litigation activity on behalf of the State, or any of its subdivisions under this Section, must be coordinated with the Department of Attorney General. In the event the insurer's attorney represents the State under this Section, the insurer's attorney may be required to be designated as a Special Assistant Attorney General by the Attorney General of the State of Michigan.
- (c) If Contractor does not deliver a Notice of Election relating to any claim of which it is notified by the State as provided above, the State may defend the claim in the manner as it may deem appropriate, at the cost and expense of Contractor. If it is determined that the claim was one against which

Contractor was required to indemnify the State, upon request of the State, Contractor must promptly reimburse the State for all the reasonable costs and expenses.

2.150 Termination/Cancellation

2.151 NOTICE AND RIGHT TO CURE

If the Contractor breaches the contract, and the State in its sole discretion determines that the breach is curable, then the State shall provide the Contractor with written notice of the breach and a time period (not less than 30 days) to cure the Breach. The notice of breach and opportunity to cure is inapplicable for successive or repeated breaches or if the State determines in its sole discretion that the breach poses a serious and imminent threat to the health or safety of any person or the imminent loss, damage, or destruction of any real or tangible personal property.

2.152 TERMINATION FOR CAUSE

- (a) The State may terminate this contract, for cause, by notifying the Contractor in writing, if the Contractor (i) breaches any of its material duties or obligations under this Contract (including a Chronic Failure to meet any particular SLA), or (ii) fails to cure a breach within the time period specified in the written notice of breach provided by the State
- (b) If this Contract is terminated for cause, the Contractor must pay all costs incurred by the State in terminating this Contract, including but not limited to, State administrative costs, reasonable attorneys' fees and court costs, and any reasonable additional costs the State may incur to procure the Services/Deliverables required by this Contract from other sources. Re-procurement costs are not consequential, indirect or incidental damages, and cannot be excluded by any other terms otherwise included in this Contract, provided the costs are not in excess of 50% more than the prices for the Service/Deliverables provided under this Contract.
- (c) If the State chooses to partially terminate this Contract for cause, charges payable under this Contract shall be equitably adjusted to reflect those Services/Deliverables that are terminated and the State must pay for all Services/Deliverables for which Final Acceptance has been granted provided up to the termination date. Services and related provisions of this Contract that are terminated for cause must cease on the effective date of the termination.
- (d) If the State terminates this Contract for cause under this Section, and it is determined, for any reason, that Contractor was not in breach of contract under the provisions of this section, that termination for cause must be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties must be limited to that otherwise provided in this Contract for a termination for convenience.

2.153 TERMINATION FOR CONVENIENCE

The State may terminate this Contract for its convenience, in whole or part, if the State determines that a termination is in the State's best interest. Reasons for the termination must be left to the sole discretion of the State and may include, but not necessarily be limited to (a) the State no longer needs the Services or products specified in the Contract, (b) relocation of office, program changes, changes in laws, rules, or regulations make implementation of the Services no longer practical or feasible, (c) unacceptable prices for Additional Services or New Work requested by the State, or (d) falsification or misrepresentation, by inclusion or non-inclusion, of information material to a response to any RFP issued by the State. The State may terminate this Contract for its convenience, in whole or in part, by giving Contractor written notice at least 30 days before the date of termination. If the State chooses to terminate this Contract in part, the charges payable under this Contract must be equitably adjusted to reflect those Services/Deliverables that are terminated. Services and related provisions of this Contract that are terminated for convenience must cease on the effective date of the termination.

2.154 TERMINATION FOR NON-APPROPRIATION

- (a) Contractor acknowledges that, if this Contract extends for several fiscal years, continuation of this Contract is subject to appropriation or availability of funds for this Contract. If funds to enable the State to effect continued payment under this Contract are not appropriated or otherwise made

available, the State must terminate this Contract and all affected Statements of Work, in whole or in part, at the end of the last period for which funds have been appropriated or otherwise made available by giving written notice of termination to Contractor. The State must give Contractor at least 30 days advance written notice of termination for non-appropriation or unavailability (or the time as is available if the State receives notice of the final decision less than 30 days before the funding cutoff).

- (b) If funding for the Contract is reduced by law, or funds to pay Contractor for the agreed-to level of the Services or production of Deliverables to be provided by Contractor are not appropriated or otherwise unavailable, the State may, upon 30 days written notice to Contractor, reduce the level of the Services or change the production of Deliverables in the manner and for the periods of time as the State may elect. The charges payable under this Contract shall be equitably adjusted to reflect any equipment, services or commodities not provided by reason of the reduction.
- (c) If the State terminates this Contract, eliminates certain Deliverables, or reduces the level of Services to be provided by Contractor under this Section, the State must pay Contractor for all Work-in-Process performed through the effective date of the termination or reduction in level, as the case may be and as determined by the State, to the extent funds are available. This Section shall not preclude Contractor from reducing or stopping Services/Deliverables or raising against the State in a court of competent jurisdiction, any claim for a shortfall in payment for Services performed or Deliverables finally accepted before the effective date of termination.

2.155 TERMINATION FOR CRIMINAL CONVICTION

The State may terminate this Contract immediately and without further liability or penalty in the event Contractor, an officer of Contractor, or an owner of a 25% or greater share of Contractor is convicted of a criminal offense related to a State, public or private Contract or subcontract.

2.156 TERMINATION FOR APPROVALS RESCINDED

The State may terminate this Contract if any final administrative or judicial decision or adjudication disapproves a previously approved request for purchase of personal services under Constitution 1963, Article 11, § 5, and Civil Service Rule 7-1. In that case, the State shall pay the Contractor for only the work completed to that point under the Contract. Termination may be in whole or in part and may be immediate as of the date of the written notice to Contractor or may be effective as of the date stated in the written notice.

2.157 RIGHTS AND OBLIGATIONS UPON TERMINATION

- (a) If the State terminates this Contract for any reason, the Contractor must (a) stop all work as specified in the notice of termination, (b) take any action that may be necessary, or that the State may direct, for preservation and protection of Deliverables or other property derived or resulting from this Contract that may be in Contractor's possession, (c) return all materials and property provided directly or indirectly to Contractor by any entity, agent or employee of the State, (d) transfer title in, and deliver to, the State, unless otherwise directed, all Deliverables intended to be transferred to the State at the termination of the Contract and which are resulting from the Contract (which must be provided to the State on an "As-Is" basis except to the extent the amounts paid by the State in respect of the items included compensation to Contractor for the provision of warranty services in respect of the materials), and (e) take any action to mitigate and limit any potential damages, or requests for Contractor adjustment or termination settlement costs, to the maximum practical extent, including terminating or limiting as otherwise applicable those subcontracts and outstanding orders for material and supplies resulting from the terminated Contract.
- (b) If the State terminates this Contract before its expiration for its own convenience, the State must pay Contractor for all charges due for Services provided before the date of termination and, if applicable, as a separate item of payment under this Contract, for Work In Process, on a percentage of completion basis at the level of completion determined by the State. All completed or partially completed Deliverables prepared by Contractor under this Contract, at the option of the State, becomes the State's property, and Contractor is entitled to receive equitable fair compensation for the Deliverables. Regardless of the basis for the termination, the State is not obligated to pay, or otherwise compensate, Contractor for any lost expected future profits, costs or expenses incurred with respect to Services not actually performed for the State.

- (c) Upon a good faith termination, the State may assume, at its option, any subcontracts and agreements for services and deliverables provided under this Contract, and may further pursue completion of the Services/Deliverables under this Contract by replacement contract or otherwise as the State may in its sole judgment deem expedient.

2.158 RESERVATION OF RIGHTS

Any termination of this Contract or any Statement of Work issued under it by a party must be with full reservation of, and without prejudice to, any rights or remedies otherwise available to the party with respect to any claims arising before or as a result of the termination.

2.160 Termination by Contractor

2.161 TERMINATION BY CONTRACTOR

If the State breaches the Contract, and the Contractor in its sole discretion determines that the breach is curable, then the Contractor will provide the State with written notice of the breach and a time period (not less than 30 days) to cure the breach. The Notice of Breach and opportunity to cure is inapplicable for successive and repeated breaches.

The Contractor may terminate this Contract if the State (i) materially breaches its obligation to pay the Contractor undisputed amounts due and owing under this Contract, (ii) breaches its other obligations under this Contract to an extent that makes it impossible or commercially impractical for the Contractor to perform the Services, or (iii) does not cure the breach within the time period specified in a written notice of breach. But the Contractor must discharge its obligations under **Section 2.160** before it terminates the Contract.

2.170 Transition Responsibilities

2.171 CONTRACTOR TRANSITION RESPONSIBILITIES

If the State terminates this contract, for convenience or cause, or if the Contract is otherwise dissolved, voided, rescinded, nullified, expires or rendered unenforceable, the Contractor shall comply with direction provided by the State to assist in the orderly transition of equipment, services, software, leases, etc. to the State or a third party designated by the State. If this Contract expires or terminates, the Contractor agrees to make all reasonable efforts to effect an orderly transition of services within a reasonable period of time that in no event will exceed 30 days. These efforts must include, but are not limited to, those listed in **Section 2.150**.

2.172 CONTRACTOR PERSONNEL TRANSITION

The Contractor shall work with the State, or a specified third party, to develop a transition plan setting forth the specific tasks and schedule to be accomplished by the parties, to effect an orderly transition. The Contractor must allow as many personnel as practicable to remain on the job to help the State, or a specified third party, maintain the continuity and consistency of the services required by this Contract. In addition, during or following the transition period, in the event the State requires the Services of the Contractor's subcontractors or vendors, as necessary to meet its needs, Contractor agrees to reasonably, and with good-faith, work with the State to use the Services of Contractor's subcontractors or vendors. Contractor will notify all of Contractor's subcontractors of procedures to be followed during transition.

2.173 CONTRACTOR INFORMATION TRANSITION

The Contractor shall provide reasonable detailed specifications for all Services/Deliverables needed by the State, or specified third party, to properly provide the Services/Deliverables required under this Contract. The Contractor will provide the State with asset management data generated from the inception of this Contract through the date on which this Contractor is terminated in a comma-delineated format unless otherwise requested by the State. The Contractor will deliver to the State any remaining

owed reports and documentation still in Contractor's possession subject to appropriate payment by the State.

2.174 CONTRACTOR SOFTWARE TRANSITION

The Contractor shall reasonably assist the State in the acquisition of any Contractor software required to perform the Services/use the Deliverables under this Contract. This must include any documentation being used by the Contractor to perform the Services under this Contract. If the State transfers any software licenses to the Contractor, those licenses must, upon expiration of the Contract, transfer back to the State at their current revision level. Upon notification by the State, Contractor may be required to freeze all non-critical changes to Deliverables/Services.

2.175 TRANSITION PAYMENTS

If the transition results from a termination for any reason, the termination provisions of this Contract must govern reimbursement. If the transition results from expiration, the Contractor will be reimbursed for all reasonable transition costs (i.e. costs incurred within the agreed period after contract expiration that result from transition operations) at the rates agreed upon by the State. The Contractor will prepare an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

2.176 STATE TRANSITION RESPONSIBILITIES

In the event that this Contract is terminated, dissolved, voided, rescinded, nullified, or otherwise rendered unenforceable, the State agrees to reconcile all accounts between the State and the Contractor, complete any pending post-project reviews and perform any others obligations upon which the State and the Contractor agree.

- (a) Reconciling all accounts between the State and the Contractor;
- (b) Completing any pending post-project reviews.

2.180 Stop Work

2.181 STOP WORK ORDERS

The State may, at any time, by written Stop Work Order to Contractor, require that Contractor stop all, or any part, of the work called for by the Contract for a period of up to 90 calendar days after the Stop Work Order is delivered to Contractor, and for any further period to which the parties may agree. The Stop Work Order must be identified as a Stop Work Order and must indicate that it is issued under this **Section**. Upon receipt of the stop work order, Contractor must immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work stoppage. Within the period of the stop work order, the State must either: (a) cancel the stop work order; or (b) terminate the work covered by the Stop Work Order as provided in **Section 2.182**.

2.182 CANCELLATION OR EXPIRATION OF STOP WORK ORDER

The Contractor shall resume work if the State cancels a Stop Work Order or if it expires. The parties shall agree upon an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract shall be modified, in writing, accordingly, if: (a) the Stop Work Order results in an increase in the time required for, or in Contractor's costs properly allocable to, the performance of any part of the Contract; and (b) Contractor asserts its right to an equitable adjustment within 30 calendar days after the end of the period of work stoppage; provided that, if the State decides the facts justify the action, the State may receive and act upon a Contractor proposal submitted at any time before final payment under the Contract. Any adjustment will conform to the requirements of **Section 2.024**.

2.183 ALLOWANCE OF CONTRACTOR COSTS

If the Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated for reasons other than material breach, the termination shall be deemed to be a termination for convenience under **Section 2.153**, and the State shall pay reasonable costs resulting from the Stop Work Order in

arriving at the termination settlement. For the avoidance of doubt, the State shall not be liable to Contractor for loss of profits because of a Stop Work Order issued under this Section.

2.190 Dispute Resolution

2.191 IN GENERAL

Any claim, counterclaim, or dispute between the State and Contractor arising out of or relating to the Contract or any Statement of Work must be resolved as follows. For all Contractor claims seeking an increase in the amounts payable to Contractor under the Contract, or the time for Contractor's performance, Contractor must submit a letter, together with all data supporting the claims, executed by Contractor's Contract Administrator or the Contract Administrator's designee certifying that (a) the claim is made in good faith, (b) the amount claimed accurately reflects the adjustments in the amounts payable to Contractor or the time for Contractor's performance for which Contractor believes the State is liable and covers all costs of every type to which Contractor is entitled from the occurrence of the claimed event, and (c) the claim and the supporting data are current and complete to Contractor's best knowledge and belief.

2.192 INFORMAL DISPUTE RESOLUTION

(a) All disputes between the parties shall be resolved under the Contract Management procedures in this Contract. If the parties are unable to resolve any dispute after compliance with the processes, the parties must meet with the Director of Procurement, DTMB, or designee, to resolve the dispute without the need for formal legal proceedings, as follows:

(1) The representatives of Contractor and the State must meet as often as the parties reasonably deem necessary to gather and furnish to each other all information with respect to the matter at issue which the parties believe to be appropriate and germane in connection with its resolution. The representatives shall discuss the problem and negotiate in good faith in an effort to resolve the dispute without the necessity of any formal proceeding.

(2) During the course of negotiations, all reasonable requests made by one party to another for non-privileged information reasonably related to the Contract shall be honored in order that each of the parties may be fully advised of the other's position.

(3) The specific format for the discussions shall be left to the discretion of the designated State and Contractor representatives, but may include the preparation of agreed upon statements of fact or written statements of position.

(4) Following the completion of this process within 60 calendar days, the Director of Procurement, DTMB, or designee, shall issue a written opinion regarding the issue(s) in dispute within 30 calendar days. The opinion regarding the dispute must be considered the State's final action and the exhaustion of administrative remedies.

(b) This Section shall not be construed to prevent either party from instituting, and a party is authorized to institute, formal proceedings earlier to avoid the expiration of any applicable limitations period, to preserve a superior position with respect to other creditors, or under Section 2.193.

(c) The State shall not mediate disputes between the Contractor and any other entity, except state agencies, concerning responsibility for performance of work under the Contract.

2.193 INJUNCTIVE RELIEF

A claim between the State and the Contractor is not subject to the provisions of Section 2.192, Informal Dispute Resolution, where a party makes a good faith determination that a breach of the Contract by the other party will result in damages so immediate, so large or severe, and so incapable of adequate redress that a temporary restraining order or other injunctive relief is the only adequate remedy.

2.194 CONTINUED PERFORMANCE

Each party agrees to continue performing its obligations under the Contract while a dispute is being resolved except to the extent the issue in dispute precludes performance (dispute over payment must not be deemed to preclude performance) and without limiting either party's right to terminate the Contract as provided in **Section 2.150**, as the case may be.

2.200 Federal and State Contract Requirements

2.201 NONDISCRIMINATION

In the performance of the Contract, Contractor agrees not to discriminate against any employee or applicant for employment, with respect to his or her hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of race, color, religion, national origin, ancestry, age, sex, height, weight, and marital status, physical or mental disability. Contractor further agrees that every subcontract entered into for the performance of this Contract or any purchase order resulting from this Contract will contain a provision requiring non-discrimination in employment, as specified here, binding upon each Subcontractor. This covenant is required under the Elliot Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, et seq., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., and any breach of this provision may be regarded as a material breach of the Contract.

2.202 UNFAIR LABOR PRACTICES

Under 1980 PA 278, MCL 423.321, et seq., the State shall not award a Contract or subcontract to an employer whose name appears in the current register of employers failing to correct an unfair labor practice compiled under section 2 of the Act. This information is compiled by the United States National Labor Relations Board. A Contractor of the State, in relation to the Contract, shall not enter into a contract with a Subcontractor, manufacturer, or supplier whose name appears in this register. Under section 4 of 1980 PA 278, MCL 423.324, the State may void any Contract if, after award of the Contract, the name of Contractor as an employer or the name of the Subcontractor, manufacturer or supplier of Contractor appears in the register.

2.203 WORKPLACE SAFETY AND DISCRIMINATORY HARASSMENT

In performing Services for the State, the Contractor shall comply with the Department of Civil Services Rule 2-20 regarding Workplace Safety and Rule 1-8.3 regarding Discriminatory Harassment. In addition, the Contractor shall comply with Civil Service regulations and any applicable agency rules provided to the Contractor. For Civil Service Rules, see <http://www.mi.gov/mdcs/0,1607,7-147-6877---,00.html>.

2.204 PREVAILING WAGE

Wages rates and fringe benefits to be paid each class of individuals employed by the Contractor, its subcontractors, their subcontractors, and all persons involved with the performance of this Contract in privity of contract with the Contractor shall not be less than the wage rates and fringe benefits established by the Michigan Department of Licensing and Regulatory Affairs, Wage and Hour Division, schedule of occupational classification and wage rates and fringe benefits for the local where the work is to be performed. The term Contractor shall include all general contractors, prime contractors, project managers, trade contractors, and all of their contractors or subcontractors and persons in privity of contract with them.

The Contractor, its subcontractors, their subcontractors and all persons involved with the performance of this contract in privity of contract with the Contractor shall keep posted on the work site, in a conspicuous place, a copy of all wage rates and fringe benefits as prescribed in the Contract. Contractor shall also post, in a conspicuous place, the address and telephone number of the Michigan Department of Licensing and Regulatory Affairs, the agency responsible for enforcement of the wage rates and fringe benefits. Contractor shall keep an accurate record showing the name and occupation of the actual wage and benefits paid to each individual employed in connection with this contract. This record shall be available to the State upon request for reasonable inspection.

If any trade is omitted from the list of wage rates and fringe benefits to be paid to each class of individuals by the Contractor, it is understood that the trades omitted shall also be paid not less than the wage rate and fringe benefits prevailing in the local where the work is to be performed.

2.210 Governing Law

2.211 GOVERNING LAW

The Contract shall in all respects be governed by, and construed according to, the substantive laws of the State of Michigan without regard to any Michigan choice of law rules that would apply the substantive law of any other jurisdiction to the extent not inconsistent with, or pre-empted by federal law.

2.212 COMPLIANCE WITH LAWS

Contractor shall comply with all applicable state, federal and local laws and ordinances in providing the Services/Deliverables.

2.213 JURISDICTION

Any dispute arising from the Contract shall be resolved in the State of Michigan. With respect to any claim between the parties, Contractor consents to venue in Ingham County, Michigan, and irrevocably waives any objections it may have to the jurisdiction on the grounds of lack of personal jurisdiction of the court or the laying of venue of the court or on the basis of forum non conveniens or otherwise. Contractor agrees to appoint agents in the State of Michigan to receive service of process.

2.220 Limitation of Liability

2.221 LIMITATION OF LIABILITY

Neither the Contractor nor the State is liable to each other, regardless of the form of action, for consequential, incidental, indirect, or special damages. This limitation of liability does not apply to claims for infringement of United States patent, copyright, trademark or trade secrets; to claims for personal injury or damage to property caused by the gross negligence or willful misconduct of the Contractor; to claims covered by other specific provisions of this Contract calling for liquidated damages; or to court costs or attorneys' fees awarded by a court in addition to damages after litigation based on this Contract.

2.230 Disclosure Responsibilities

2.231 DISCLOSURE OF LITIGATION

Contractor shall disclose any material criminal litigation, investigations or proceedings involving the Contractor (and each Subcontractor) or any of its officers or directors or any litigation, investigations or proceedings under the Sarbanes-Oxley Act. In addition, each Contractor (and each Subcontractor) shall notify the State of any material civil litigation, arbitration or proceeding which arises during the term of the Contract and extensions, to which Contractor (or, to the extent Contractor is aware, any Subcontractor) is a party, and which involves: (i) disputes that might reasonably be expected to adversely affect the viability or financial stability of Contractor or any Subcontractor; or (ii) a claim or written allegation of fraud against Contractor or, to the extent Contractor is aware, any Subcontractor by a governmental or public entity arising out of their business dealings with governmental or public entities. The Contractor shall disclose in writing to the Contract Administrator any litigation, investigation, arbitration or other proceeding (collectively, "Proceeding") within 30 days of its occurrence. Details of settlements that are prevented from disclosure by the terms of the settlement may be annotated. Information provided to the State from Contractor's publicly filed documents referencing its material litigation shall be deemed to satisfy the requirements of this Section.

If any Proceeding disclosed to the State under this Section, or of which the State otherwise becomes aware, during the term of this Contract would cause a reasonable party to be concerned about:

- (a) the ability of Contractor (or a Subcontractor) to continue to perform this Contract according to its terms and conditions, or
- (b) whether Contractor (or a Subcontractor) in performing Services for the State is engaged in conduct which is similar in nature to conduct alleged in the Proceeding, which conduct would constitute a breach of this Contract or a violation of Michigan law, regulations or public policy, then the Contractor must provide the State all reasonable assurances requested by the State to demonstrate that:
 - (1) Contractor and its Subcontractors will be able to continue to perform this Contract and any Statements of Work according to its terms and conditions, and
 - (2) Contractor and its Subcontractors have not and will not engage in conduct in performing the Services which is similar in nature to the conduct alleged in the Proceeding.
- (c) Contractor shall make the following notifications in writing:
 - (1) Within 30 days of Contractor becoming aware that a change in its ownership or officers has occurred, or is certain to occur, or a change that could result in changes in the valuation of its capitalized assets in the accounting records, Contractor must notify DTMB-Procurement.
 - (2) Contractor shall also notify DTMB Procurement within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership or officers.
 - (3) Contractor shall also notify DTMB-Procurement within 30 days whenever changes to company affiliations occur.

2.232 CALL CENTER DISCLOSURE

Contractor and/or all subcontractors involved in the performance of this Contract providing call or contact center services to the State shall disclose the location of its call or contact center services to inbound callers. Failure to disclose this information is a material breach of this Contract.

2.233 BANKRUPTCY

The State may, without prejudice to any other right or remedy, terminate this Contract, in whole or in part, and, at its option, may take possession of the "Work in Process" and finish the Works in Process by whatever appropriate method the State may deem expedient if:

- (a) the Contractor files for protection under the bankruptcy laws;
- (b) an involuntary petition is filed against the Contractor and not removed within 30 days;
- (c) the Contractor becomes insolvent or if a receiver is appointed due to the Contractor's insolvency;
- (d) the Contractor makes a general assignment for the benefit of creditors; or
- (e) the Contractor or its affiliates are unable to provide reasonable assurances that the Contractor or its affiliates can deliver the services under this Contract.

Contractor will fix appropriate notices or labels on the Work in Process to indicate ownership by the State. To the extent reasonably possible, materials and Work in Process shall be stored separately from other stock and marked conspicuously with labels indicating ownership by the State.

2.240 Performance

2.241 TIME OF PERFORMANCE

- (a) Contractor shall use commercially reasonable efforts to provide the resources necessary to complete all Services and Deliverables according to the time schedules contained in the Statements of Work and other Exhibits governing the work, and with professional quality.
- (b) Without limiting the generality of **Section 2.241**, Contractor shall notify the State in a timely manner upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion of any Deliverables/Services on the scheduled due dates in the latest State-approved delivery schedule and must inform the State of the projected actual delivery date.

- (c) If the Contractor believes that a delay in performance by the State has caused or will cause the Contractor to be unable to perform its obligations according to specified Contract time periods, the Contractor must notify the State in a timely manner and must use commercially reasonable efforts to perform its obligations according to the Contract time periods notwithstanding the State's failure. Contractor will not be in default for a delay in performance to the extent the delay is caused by the State.

2.242 SERVICE LEVEL AGREEMENT (SLA)

- (a) SLAs will be completed with the following operational considerations:
- (1) SLAs will not be calculated for individual Incidents where any event of Excusable Failure has been determined; Incident means any interruption in Services.
 - (2) SLAs will not be calculated for individual Incidents where loss of service is planned and where the State has received prior notification or coordination.
 - (3) SLAs will not apply if the applicable Incident could have been prevented through planning proposed by Contractor and not implemented at the request of the State. To invoke this consideration, complete documentation relevant to the denied planning proposal must be presented to substantiate the proposal.
 - (4) Time period measurements will be based on the time Incidents are received by the Contractor and the time that the State receives notification of resolution based on 24x7x365 time period, except that the time period measurement will be suspended based on the following:
 - (i) Time period(s) will not apply where Contractor does not have access to a physical State Location and where access to the State Location is necessary for problem identification and resolution.
 - (ii) Time period(s) will not apply where Contractor needs to obtain timely and accurate information or appropriate feedback and is unable to obtain timely and accurate information or appropriate feedback from the State.
- (b) Chronic Failure for any Service(s) will be defined as three unscheduled outage(s) or interruption(s) on any individual Service for the same reason or cause or if the same reason or cause was reasonably discoverable in the first instance over a rolling 30 day period. Chronic Failure will result in the State's option to terminate the effected individual Service(s) and procure them from a different vendor for the chronic location(s) with Contractor to pay the difference in charges for up to three additional months. The termination of the Service will not affect any tiered pricing levels.
- (c) Root Cause Analysis will be performed on any Business Critical outage(s) or outage(s) on Services when requested by the Contract Administrator. Contractor will provide its analysis within two weeks of outage(s) and provide a recommendation for resolution.
- (d) All decimals must be rounded to two decimal places with five and greater rounding up and four and less rounding down unless otherwise specified.

2.243 LIQUIDATED DAMAGES

The parties acknowledge that late or improper completion of the Work will cause loss and damage to the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result. Therefore, Contractor and the State agree that if there is late or improper completion of the Work and the State does not elect to exercise its rights under **Section 2.152**, the State is entitled to collect liquidated damages in the amount of \$5,000.00 and an additional \$100.00 per day for each day Contractor fails to remedy the late or improper completion of the Work.

Unauthorized Removal of any Key Personnel

It is acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of the Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 2.152**, the State may assess liquidated damages against Contractor as specified below.

For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the liquidated damages amount is \$25,000.00 per individual if the Contractor identifies a replacement

approved by the State under **Section 2.060** and assigns the replacement to the Project to shadow the Key Personnel who is leaving for a period of at least 30 days before the Key Personnel's removal.

If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 days, in addition to the \$25,000.00 liquidated damages for an Unauthorized Removal, Contractor must pay the amount of \$833.33 per day for each day of the 30 day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to \$25,000.00 maximum per individual. The total liquidated damages that may be assessed per Unauthorized Removal and failure to provide 30 days of shadowing must not exceed \$50,000.00 per individual.

2.244 EXCUSABLE FAILURE

Neither party will be liable for any default, damage or delay in the performance of its obligations under the Contract to the extent the default, damage or delay is caused by government regulations or requirements (executive, legislative, judicial, military or otherwise), power failure, electrical surges or current fluctuations, lightning, earthquake, war, water or other forces of nature or acts of God, delays or failures of transportation, equipment shortages, suppliers' failures, or acts or omissions of common carriers, fire; riots, civil disorders; strikes or other labor disputes, embargoes; injunctions (provided the injunction was not issued as a result of any fault or negligence of the party seeking to have its default or delay excused); or any other cause beyond the reasonable control of a party; provided the non-performing party and its Subcontractors are without fault in causing the default or delay, and the default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of alternate sources, workaround plans or other means, including disaster recovery plans.

If a party does not perform its contractual obligations for any of the reasons listed above, the non-performing party will be excused from any further performance of its affected obligation(s) for as long as the circumstances prevail. But the party must use commercially reasonable efforts to recommence performance whenever and to whatever extent possible without delay. A party must promptly notify the other party in writing immediately after the excusable failure occurs, and also when it abates or ends.

If any of the above-enumerated circumstances substantially prevent, hinder, or delay the Contractor's performance of the Services/provision of Deliverables for more than 10 Business Days, and the State determines that performance is not likely to be resumed within a period of time that is satisfactory to the State in its reasonable discretion, then at the State's option: (a) the State may procure the affected Services/Deliverables from an alternate source, and the State is not be liable for payment for the unperformed Services/ Deliverables not provided under the Contract for so long as the delay in performance continues; (b) the State may terminate any portion of the Contract so affected and the charges payable will be equitably adjusted to reflect those Services/Deliverables terminated; or (c) the State may terminate the affected Statement of Work without liability to Contractor as of a date specified by the State in a written notice of termination to the Contractor, except to the extent that the State must pay for Services/Deliverables provided through the date of termination.

The Contractor will not have the right to any additional payments from the State as a result of any Excusable Failure occurrence or to payments for Services not rendered/Deliverables not provided as a result of the Excusable Failure condition. Defaults or delays in performance by Contractor which are caused by acts or omissions of its Subcontractors will not relieve Contractor of its obligations under the Contract except to the extent that a Subcontractor is itself subject to an Excusable Failure condition described above and Contractor cannot reasonably circumvent the effect of the Subcontractor's default or delay in performance through the use of alternate sources, workaround plans or other means.

2.250 Approval of Deliverables

2.251 DELIVERY OF DELIVERABLES

A list of the Deliverables to be prepared and delivered by Contractor including, for each Deliverable, the scheduled delivery date and a designation of whether the Deliverable is a document ("Written Deliverable") or a Custom Software Deliverable is attached, if applicable. All Deliverables shall be completed and delivered for State review and written approval and, where applicable, installed in accordance with the State-approved delivery schedule and any other applicable terms and conditions of this Contract.

Prior to delivering any Deliverable to the State, Contractor will first perform all required quality assurance activities, and, in the case of Custom Software Deliverables, System Testing to verify that the Deliverable is complete and in conformance with its specifications. Before delivering a Deliverable to the State, Contractor shall certify to the State that (1) it has performed such quality assurance activities, (2) it has performed any applicable testing, (3) it has corrected all material deficiencies discovered during such quality assurance activities and testing, (4) the Deliverable is in a suitable state of readiness for the State's review and approval, and (5) the Deliverable/Service has all Critical Security patches/updates applied.

In discharging its obligations under this Section, Contractor shall be at all times (except where the parties agree otherwise in writing) in compliance with Level 3 of the Software Engineering Institute's Capability Maturity Model for Software ("CMM Level 3") or its equivalent.

2.252 CONTRACTOR SYSTEM TESTING

Contractor will be responsible for System Testing each Custom Software Deliverable in Contractor's development environment prior to turning over the Custom Software Deliverable to the State for User Acceptance Testing and approval. Contractor's System Testing shall include the following, at a minimum, plus any other testing required by CMM Level 3 or Contractor's system development methodology:

Contractor will be responsible for performing Unit Testing and incremental Integration Testing of the components of each Custom Software Deliverable.

Contractor's System Testing will also include Integration Testing of each Custom Software Deliverable to ensure proper inter-operation with all prior software Deliverables, interfaces and other components that are intended to inter-operate with such Custom Software Deliverable, and will include Regression Testing, volume and stress testing to ensure that the Custom Software Deliverables are able to meet the State's projected growth in the number and size of transactions to be processed by the Application and number of users, as such projections are set forth in the applicable Statement of Work.

Contractor's System Testing will also include Business Function Testing and Technical Testing of each Application in a simulated production environment. Business Function Testing will include testing of full work streams that flow through the Application as the Application will be incorporated within the State's computing environment. The State shall participate in and provide support for the Business Function Testing to the extent reasonably requested by Contractor. Within ten (10) days before the commencement of Business Function Testing pursuant to this Section, Contractor shall provide the State for State review and written approval Contractor's test plan for Business Function Testing.

Within five (5) Business Days following the completion of System Testing pursuant to this **Section**, Contractor shall provide to the State a testing matrix establishing that testing for each condition identified in the System Testing plans has been conducted and successfully concluded. To the extent that testing occurs on State premises, the State shall be entitled to observe or otherwise participate in testing under this Section as the State may elect.

2.253 APPROVAL OF DELIVERABLES, IN GENERAL

All Deliverables (Written Deliverables and Custom Software Deliverables) require formal written approval by the State, in accordance with the following procedures. Formal approval by the State requires that the Deliverable be confirmed in writing by the State to meet its specifications, which, in the case of Custom Software Deliverables, will include the successful completion of State User Acceptance Testing, to be led by the State with the support and assistance of Contractor. The parties acknowledge that the approval

process set forth herein will be facilitated by ongoing consultation between the parties, visibility of interim and intermediate Deliverables and collaboration on key decisions.

The State's obligation to comply with any State Review Period is conditioned on the timely delivery of Deliverables being reviewed. If Contractor fails to provide a Deliverable to the State in a timely manner, the State will nevertheless use commercially reasonable efforts to complete its review or testing within the applicable State Review Period.

Before commencement of its review or testing of a Deliverable, the State may inspect the Deliverable to confirm that all components of the Deliverable (e.g., software, associated documentation, and other materials) have been delivered. If the State determines that the Deliverable is incomplete, the State may refuse delivery of the Deliverable without performing any further inspection or testing of the Deliverable. Otherwise, the review period will be deemed to have started on the day the State receives the Deliverable and the applicable certification by Contractor in accordance with this Section.

The State will approve in writing a Deliverable upon confirming that it conforms to and, in the case of a Custom Software Deliverable, performs in accordance with, its specifications without material deficiency. The State may, but shall not be required to, conditionally approve in writing a Deliverable that contains material deficiencies if the State elects to permit Contractor to rectify them post-approval. In any case, Contractor will be responsible for working diligently to correct within a reasonable time at Contractor's expense all deficiencies in the Deliverable that remain outstanding at the time of State approval.

If, after three (3) opportunities (the original and two repeat efforts), Contractor is unable to correct all deficiencies preventing State approval of a Deliverable, the State may: (i) demand that Contractor cure the failure and give Contractor additional time to cure the failure at the sole expense of Contractor; or (ii) keep this Contract in force and do, either itself or through other parties, whatever Contractor has failed to do, in which event Contractor shall bear any excess expenditure incurred by the State in so doing beyond the contract price for such Deliverable and will pay the State an additional sum equal to ten percent (10%) of such excess expenditure to cover the State's general expenses without the need to furnish proof in substantiation of such general expenses; or (iii) terminate this Contract for default, either in whole or in part by notice to Contractor (and without the need to afford Contractor any further opportunity to cure). Notwithstanding the foregoing, the State shall not use, as a basis for exercising its termination rights under this Section, deficiencies discovered in a repeat State Review Period that could reasonably have been discovered during a prior State Review Period.

The State, at any time and in its own discretion, may halt the UAT or approval process if such process reveals deficiencies in or problems with a Deliverable in a sufficient quantity or of a sufficient severity as to make the continuation of such process unproductive or unworkable. In such case, the State may return the applicable Deliverable to Contractor for correction and re-delivery prior to resuming the review or UAT process and, in that event, Contractor will correct the deficiencies in such Deliverable in accordance with the Contract, as the case may be.

Approval in writing of a Deliverable by the State shall be provisional; that is, such approval shall not preclude the State from later identifying deficiencies in, and declining to accept, a subsequent Deliverable based on or which incorporates or inter-operates with an approved Deliverable, to the extent that the results of subsequent review or testing indicate the existence of deficiencies in the subsequent Deliverable, or if the Application of which the subsequent Deliverable is a component otherwise fails to be accepted pursuant to **Section 2.080**.

2.254 PROCESS FOR APPROVAL OF WRITTEN DELIVERABLES

The State Review Period for Written Deliverables will be the number of days set forth in the applicable Statement of Work following delivery of the final version of the Written Deliverable (failing which the State Review Period, by default, shall be five (5) Business Days for Written Deliverables of one hundred (100) pages or less and ten (10) Business Days for Written Deliverables of more than one hundred (100) pages). The duration of the State Review Periods will be doubled if the State has not had an opportunity to review an interim draft of the Written Deliverable prior to its submission to the State. The State agrees to notify Contractor in writing by the end of the State Review Period either stating that the Written

Deliverable is approved in the form delivered by Contractor or describing any deficiencies that shall be corrected prior to approval of the Written Deliverable (or at the State's election, subsequent to approval of the Written Deliverable). If the State delivers to Contractor a notice of deficiencies, Contractor will correct the described deficiencies and within five (5) Business Days resubmit the Deliverable in a form that shows all revisions made to the original version delivered to the State. Contractor's correction efforts will be made at no additional charge. Upon receipt of a corrected Written Deliverable from Contractor, the State will have a reasonable additional period of time, not to exceed the length of the original State Review Period, to review the corrected Written Deliverable to confirm that the identified deficiencies have been corrected.

2.255 PROCESS FOR APPROVAL OF CUSTOM SOFTWARE DELIVERABLES

The State will conduct UAT of each Custom Software Deliverable in accordance with the following procedures to determine whether it meets the criteria for State approval – i.e., whether it conforms to and performs in accordance with its specifications without material deficiencies.

Within thirty (30) days (or such other number of days as the parties may agree to in writing) prior to Contractor's delivery of any Custom Software Deliverable to the State for approval, Contractor shall provide to the State a set of proposed test plans, including test cases, scripts, data and expected outcomes, for the State's use (which the State may supplement in its own discretion) in conducting UAT of the Custom Software Deliverable. Contractor, upon request by the State, shall provide the State with reasonable assistance and support during the UAT process.

For the Custom Software Deliverables listed in an attachment, the State Review Period for conducting UAT will be as indicated in the attachment. For any other Custom Software Deliverables not listed in an attachment, the State Review Period shall be the number of days agreed in writing by the parties (failing which it shall be forty-five (45) days by default). The State Review Period for each Custom Software Deliverable will begin when Contractor has delivered the Custom Software Deliverable to the State accompanied by the certification required by this **Section** and the State's inspection of the Deliverable has confirmed that all components of it have been delivered.

The State's UAT will consist of executing test scripts from the proposed testing submitted by Contractor, but may also include any additional testing deemed appropriate by the State. If the State determines during the UAT that the Custom Software Deliverable contains any deficiencies, the State will notify Contractor of the deficiency by making an entry in an incident reporting system available to both Contractor and the State. Contractor will modify promptly the Custom Software Deliverable to correct the reported deficiencies, conduct appropriate System Testing (including, where applicable, Regression Testing) to confirm the proper correction of the deficiencies and re-deliver the corrected version to the State for re-testing in UAT. Contractor will coordinate the re-delivery of corrected versions of Custom Software Deliverables with the State so as not to disrupt the State's UAT process. The State will promptly re-test the corrected version of the Software Deliverable after receiving it from Contractor.

Within three (3) business days after the end of the State Review Period, the State will give Contractor a written notice indicating the State's approval or rejection of the Custom Software Deliverable according to the criteria and process set out in this **Section**.

2.256 FINAL ACCEPTANCE

"Final Acceptance" shall be considered to occur when the Custom Software Deliverable to be delivered has been approved by the State and has been operating in production without any material deficiency for fourteen (14) consecutive days. If the State elects to defer putting a Custom Software Deliverable into live production for its own reasons, not based on concerns about outstanding material deficiencies in the Deliverable, the State shall nevertheless grant Final Acceptance of the Project.

2.260 Ownership

2.261 OWNERSHIP OF WORK PRODUCT BY STATE

Contractor grants to the State a royalty-free, nonexclusive, perpetual, unlimited and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use, for state government purposes, the software modifications, derivatives and improvements and associated documentation developed and/or obtained through this Contract or associated SOWs. Contractor and State understand and agree that these modifications will be included in the standard product and may be distributed to other customers.

2.262 VESTING OF RIGHTS

Intentionally left blank

2.263 RIGHTS IN DATA

The State is the owner of all data made available by the State to the Contractor or its agents, Subcontractors or representatives under the Contract. The Contractor will not use the State's data for any purpose other than providing the Services, nor will any part of the State's data be disclosed, sold, assigned, leased or otherwise disposed of to the general public or to specific third parties or commercially exploited by or on behalf of the Contractor. No employees of the Contractor, other than those on a strictly need-to-know basis, have access to the State's data. Contractor will not possess or assert any lien or other right against the State's data. Without limiting the generality of this Section, the Contractor must only use personally identifiable information as strictly necessary to provide the Services and must disclose the information only to its employees who have a strict need-to-know the information. The Contractor must comply at all times with all laws and regulations applicable to the personally identifiable information.

The State is the owner of all State-specific data under the Contract. The State may use the data provided by the Contractor for any purpose. The State will not possess or assert any lien or other right against the Contractor's data. Without limiting the generality of this Section, the State may use personally identifiable information only as strictly necessary to utilize the Services and must disclose the information only to its employees who have a strict need to know the information, except as provided by law. The State must comply at all times with all laws and regulations applicable to the personally identifiable information. Other material developed and provided to the State remains the State's sole and exclusive property.

2.264 OWNERSHIP OF MATERIALS

The State and the Contractor will continue to own their respective proprietary technologies developed before entering into the Contract. Any hardware bought through the Contractor by the State, and paid for by the State, will be owned by the State. Any software licensed through the Contractor and sold to the State, will be licensed directly to the State.

2.270 State Standards

2.271 EXISTING TECHNOLOGY STANDARDS

The Contractor must adhere to all existing standards as described within the comprehensive listing of the State's existing technology standards at <http://www.michigan.gov/dmb/0,4568,7-150-56355-108233--00.html>.

2.272 ACCEPTABLE USE POLICY

To the extent that Contractor has access to the State computer system, Contractor must comply with the State's Acceptable Use Policy, see http://michigan.gov/cybersecurity/0,1607,7-217-34395_34476---00.html. All Contractor employees must be required, in writing, to agree to the State's Acceptable Use

Policy before accessing the State system. The State reserves the right to terminate Contractor's access to the State system if a violation occurs.

2.273 SYSTEMS CHANGES

Contractor is not responsible for and not authorized to make changes to any State systems without written authorization from the Project Manager. Any changes Contractor makes to State systems with the State's approval must be done according to applicable State procedures, including security, access and configuration management procedures.

2.274 ELECTRONIC RECEIPT PROCESSING STANDARD

All electronic commerce applications that allow for electronic receipt of credit/debit card and electronic check (ACH) transactions must be processed via the Centralized Electronic Payment Authorization System (CEPAS).

2.280 Extended Purchasing Program

2.281 EXTENDED PURCHASING PROGRAM

The Contract will be extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal. Upon mutual written agreement between the State of Michigan and the Contractor, this Contract may be extended to (a) State of Michigan employees, or (b) other states (including governmental subdivisions and authorized entities).

If extended, the Contractor must supply all goods and services at the established Agreement prices and terms. The State reserves the right to negotiate additional discounts based on any increased volume generated by such extensions.

The Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

2.290 Environmental Provision

2.291 ENVIRONMENTAL PROVISION

Energy Efficiency Purchasing Policy: The State seeks wherever possible to purchase energy efficient products. This includes giving preference to U.S. Environmental Protection Agency (EPA) certified 'Energy Star' products for any category of products for which EPA has established Energy Star certification. For other purchases, the State may include energy efficiency as one of the priority factors to consider when choosing among comparable products.

Environmental Purchasing Policy: The State of Michigan is committed to encouraging the use of products and services that impact the environment less than competing products. The State is accomplishing this by including environmental considerations in purchasing decisions, while remaining fiscally responsible, to promote practices that improve worker health, conserve natural resources, and prevent pollution. Environmental components that are to be considered include recycled content and recyclables; energy efficiency; and the presence of undesirable materials in the products, especially those toxic chemicals which are persistent and bioaccumulative. The Contractor should be able to supply products containing recycled and environmentally preferable materials that meet performance requirements and is encouraged to offer such products throughout the duration of this Contract. Information on any relevant third party certification (such as Green Seal, Energy Star, etc.) should also be provided.

Hazardous Materials: For the purposes of this Section, "Hazardous Materials" is a generic term used to describe asbestos, ACBMs, PCBs, petroleum products, construction materials including paint thinners, solvents, gasoline, oil, and any other material the manufacture, use, treatment, storage, transportation or disposal of which is regulated by the federal, state or local laws governing the protection of the public health, natural resources or the environment. This includes, but is not limited to, materials the as batteries and circuit packs, and other materials that are regulated as (1) "Hazardous Materials" under the Hazardous Materials Transportation Act, (2) "chemical hazards" under the Occupational Safety and Health Administration standards, (3) "chemical substances or mixtures" under the Toxic Substances Control Act, (4) "pesticides" under the Federal Insecticide Fungicide and Rodenticide Act, and (5) "hazardous wastes" as defined or listed under the Resource Conservation and Recovery Act.

- (a) The Contractor shall use, handle, store, dispose of, process, transport and transfer any material considered a Hazardous Material according to all federal, State and local laws. The State shall provide a safe and suitable environment for performance of Contractor's Work. Before the commencement of Work, the State shall advise the Contractor of the presence at the work site of any Hazardous Material to the extent that the State is aware of the Hazardous Material. If the Contractor encounters material reasonably believed to be a Hazardous Material and which may present a substantial danger, the Contractor shall immediately stop all affected Work, notify the State in writing about the conditions encountered, and take appropriate health and safety precautions.
- (b) Upon receipt of a written notice, the State will investigate the conditions. If (a) the material is a Hazardous Material that may present a substantial danger, and (b) the Hazardous Material was not brought to the site by the Contractor, or does not result in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Materials, the State shall order a suspension of Work in writing. The State shall proceed to have the Hazardous Material removed or rendered harmless. In the alternative, the State shall terminate the affected Work for the State's convenience.
- (c) Once the Hazardous Material has been removed or rendered harmless by the State, the Contractor shall resume Work as directed in writing by the State. Any determination by the Michigan Department of Community Health or the Michigan Department of Environmental Quality that the Hazardous Material has either been removed or rendered harmless is binding upon the State and Contractor for the purposes of resuming the Work. If any incident with Hazardous Material results in delay not reasonable anticipatable under the circumstances and which is attributable to the State, the applicable SLAs for the affected Work will not be counted in a time as mutually agreed by the parties.
- (d) If the Hazardous Material was brought to the site by the Contractor, or results in whole or in part from any violation by the Contractor of any laws covering the use, handling, storage, disposal of, processing, transport and transfer of Hazardous Material, or from any other act or omission within the control of the Contractor, the Contractor shall bear its proportionate share of the delay and costs involved in cleaning up the site and removing and rendering harmless the Hazardous Material according to Applicable Laws to the condition approved by applicable regulatory agency(ies).

Labeling: Michigan has a Consumer Products Rule pertaining to labeling of certain products containing volatile organic compounds. For specific details visit http://www.michigan.gov/deq/0,1607,7-135-3310_4108-173523--,00.html

Refrigeration and Air Conditioning: The Contractor shall comply with the applicable requirements of Sections 608 and 609 of the Clean Air Act (42 U.S.C. 7671g and 7671h) as each or both apply to this contract.

Environmental Performance: Waste Reduction Program - Contractor shall establish a program to promote cost-effective waste reduction in all operations and facilities covered by this contract. The Contractor's programs shall comply with applicable Federal, State, and local requirements, specifically including Section 6002 of the Resource Conservation and Recovery Act (42 U.S.C. 6962, et seq.).

2.300 Deliverables

2.301 SOFTWARE

A list of the items of software the State is required to purchase for executing the Contract is attached. The list includes all software required to complete the Contract and make the Deliverables operable. If any additional software is required in order for the Deliverables to meet the requirements of this Contract, such software shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Statement of Work or Contract Change Notice). The attachment also identifies certain items of software to be provided by the State.

2.302 HARDWARE

A list of the items of hardware the State is required to purchase for executing the Contract is attached. The list includes all hardware required to complete the Contract and make the Deliverables operable. If any additional hardware is required in order for the Deliverables to meet the requirements of this Contract, such hardware shall be provided to the State by Contractor at no additional charge (except where agreed upon and specified in a Contract Change Notice). The attachment also identifies certain items of hardware to be provided by the State.

2.310 Software Warranties

2.311 PERFORMANCE WARRANTY

The Contractor represents and warrants that Deliverables, after Final Acceptance, will perform and operate in compliance with the requirements and other standards of performance contained in this Contract (including all descriptions, specifications and drawings made a part of the Contract) for a period of (90) ninety days. In the event of a breach of this warranty, Contractor will promptly correct the affected Deliverable(s) at no charge to the State.

2.312 NO SURREPTITIOUS CODE WARRANTY

The Contractor represents and warrants that no copy of licensed Software provided to the State contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this Contract as the "No Surreptitious Code Warranty."

As used in this Contract, "Self-Help Code" means any back door, time bomb, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

As used in this Contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code. Unauthorized Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access via modem) for purposes of maintenance or technical support.

In addition, Contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the State.

2.313 CALENDAR WARRANTY

The Contractor represents and warrants that all software for which the Contractor either sells or licenses to the State of Michigan and used by the State prior to, during or after the calendar year 2000, includes or shall include, at no added cost to the State, design and performance so the State shall not experience software abnormality and/or the generation of incorrect results from the software, due to date oriented processing, in the operation of the business of the State of Michigan.

The software design, to insure calendar year rollover compatibility, shall include, but is not limited to: data structures (databases, data files, etc.) that provide 4-digit date century; stored data that contain date century recognition, including, but not limited to, data stored in databases and hardware device internal system dates; calculations and program logic (e.g., sort algorithms, calendar generation, event recognition, and all processing actions that use or produce date values) that accommodates same century and multi-century formulas and date values; interfaces that supply data to and receive data from other systems or organizations that prevent non-compliant dates and data from entering any State system; user interfaces (i.e., screens, reports, etc.) that accurately show 4 digit years; and assurance that the year 2000 shall be correctly treated as a leap year within all calculation and calendar logic.

2.314 THIRD-PARTY SOFTWARE WARRANTY

The Contractor represents and warrants that it will disclose the use or incorporation of any third-party software into the Deliverables. At the time of Delivery, the Contractor shall provide in writing the name and use of any Third-party Software, including information regarding the Contractor's authorization to include and utilize such software. The notice shall include a copy of any ownership agreement or license that authorizes the Contractor to use the Third-party Software.

2.315 PHYSICAL MEDIA WARRANTY

Contractor represents and warrants that each licensed copy of the Software provided by the Contractor is free from physical defects in the media that tangibly embodies the copy. This warranty does not apply to defects discovered more than (30) thirty days after that date of Final Acceptance of the Software by the State. This warranty does not apply to defects arising from acts of Excusable Failure. If the Contractor breaches this warranty, then the State shall be entitled to replacement of the non-compliant copy by Contractor, at Contractor's expense (including shipping and handling).

2.320 Software Licensing

2.321 CROSS-LICENSE, DELIVERABLES ONLY, LICENSE TO CONTRACTOR

The State grants to the Contractor, the royalty-free, world-wide, non-exclusive right and license under any Deliverable now or in the future owned by the State, or with respect to which the State has a right to grant such rights or licenses, to the extent required by the Contractor to market the Deliverables and exercise its full rights in the Deliverables, including, without limitation, the right to make, use and sell products and services based on or incorporating such Deliverables.

2.322 CROSS-LICENSE, DELIVERABLES AND DERIVATIVE WORK, LICENSE TO CONTRACTOR

The State grants to the Contractor, the royalty-free, world-wide, non-exclusive right and license under any Deliverable and/or Derivative Work now or in the future owned by the State, or with respect to which the State has a right to grant such rights or licenses, to the extent required by the Contractor to market the Deliverables and/or Derivative Work and exercise its full rights in the Deliverables and/or Derivative Work, including, without limitation, the right to make, use and sell products and services based on or incorporating such Deliverables and/or Derivative Work.

2.323 LICENSE BACK TO THE STATE

Unless otherwise specifically agreed to by the State, before initiating the preparation of any Deliverable that is a Derivative of a preexisting work, the Contractor shall cause the State to have and obtain the irrevocable, nonexclusive, worldwide, royalty-free right and license to (1) use, execute, reproduce, display, perform, distribute internally or externally, sell copies of, and prepare Derivative Works based

upon all preexisting works and Derivative Works thereof, and (2) authorize or sublicense others from time to time to do any or all of the foregoing.

2.324 LICENSE RETAINED BY CONTRACTOR

Contractor grants to the State a non-exclusive, royalty-free, site-wide, irrevocable, transferable license to use the Software and related documentation according to the terms and conditions of this Contract. For the purposes of this license, "site-wide" includes any State of Michigan office regardless of its physical location.

The State may modify the Software and may combine such with other programs or materials to form a derivative work. The State will own and hold all copyright, trademarks, patent and other intellectual property rights in any derivative work, excluding any rights or interest in Software other than those granted in this Contract.

The State may copy each item of Software to multiple hard drives or networks unless otherwise agreed by the parties.

The State will make and maintain no more than one archival copy of each item of Software, and each copy will contain all legends and notices and will be subject to the same conditions and restrictions as the original. The State may also make copies of the Software in the course of routine backups of hard drive(s) for the purpose of recovery of hard drive contents.

In the event that the Contractor shall, for any reason, cease to conduct business, or cease to support the Software, the State shall have the right to convert these licenses into perpetual licenses, with rights of quiet enjoyment, but subject to payment obligations not to exceed the then current rates.

2.325 PRE-EXISTING MATERIALS FOR CUSTOM SOFTWARE DELIVERABLES

All Intellectual Property Rights connected to the Contractor's pre-existing materials such as architectural structure, modules, and processes that may be used in the work, but do not constitute the whole of the finished work shall be owned by Contractor. The State shall own a royalty-free, irrevocable, perpetual use license for these architectural structures, modules, and processes that may be used in the work, as well as the whole of the finished works.

SOM shall retain all intellectual property rights in and to all client provided materials. Contractor disclaims any rights to or interest in any SOM provided materials (or any other assets or properties of SOM.)

2.330 Source Code Escrow

2.331 DEFINITION

"Source Code Escrow Package" shall mean:

- (a) A complete copy in machine-readable form of the source code and executable code of the Licensed Software, including any updates or new releases of the product;
- (b) A complete copy of any existing design documentation and user documentation, including any updates or revisions; and/or
- (c) Complete instructions for compiling and linking every part of the source code into executable code for purposes of enabling verification of the completeness of the source code as provided below. Such instructions shall include precise identification of all compilers, library packages, and linkers used to generate executable code.

2.332 DELIVERY OF SOURCE CODE INTO ESCROW

Contractor shall deliver a Source Code Escrow Package to the Escrow Agent, pursuant to the Escrow Contract, which shall be entered into on commercially reasonable terms subject to the provisions of this Contract within (30) thirty days of the execution of this Contract.

2.333 DELIVERY OF NEW SOURCE CODE INTO ESCROW

If at anytime during the term of this Contract, the Contractor provides a maintenance release or upgrade version of the Licensed Software, Contractor shall within ten (10) days deposit with the Escrow Agent, in accordance with the Escrow Contract, a Source Code Escrow Package for the maintenance release or upgrade version, and provide the State with notice of the delivery.

2.334 VERIFICATION

The State reserves the right at any time, but not more than once a year, either itself or through a third party contractor, upon thirty (30) days written notice, to seek verification of the Source Code Escrow Package.

2.335 ESCROW FEES

The Contractor will pay all fees and expenses charged by the Escrow Agent.

2.336 RELEASE EVENTS

The Source Code Escrow Package may be released from escrow to the State, temporarily or permanently, upon the occurrence of one or more of the following:

- (a) The Contractor becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for its business or assets, becomes subject to any proceeding under bankruptcy or insolvency law, whether domestic or foreign;
- (b) The Contractor has wound up or liquidated its business voluntarily or otherwise and the State has reason to believe that such events will cause the Contractor to fail to meet its warranties and maintenance obligations in the foreseeable future;
- (c) The Contractor voluntarily or otherwise discontinues support of the provided products or fails to support the products in accordance with its maintenance obligations and warranties.

2.337 RELEASE EVENT PROCEDURES

If the State desires to obtain the Source Code Escrow Package from the Escrow Agent upon the occurrence of an Event in this **Section**, then:

- (a) The State shall comply with all procedures in the Escrow Contract;
- (b) The State shall maintain all materials and information comprising the Source Code Escrow Package in confidence in accordance with this Contract;
- (c) If the release is a temporary one, then the State shall promptly return all released materials to Contractor when the circumstances leading to the release are no longer in effect.

2.338 LICENSE

Upon release from the Escrow Agent pursuant to an event described in this **Section**, the Contractor automatically grants the State a non-exclusive, irrevocable license to use, reproduce, modify, maintain, support, update, have made, and create Derivative Works. Further, the State shall have the right to use the Source Code Escrow Package in order to maintain and support the Licensed Software so that it can be used by the State as set forth in this Contract.

2.339 DERIVATIVE WORKS

Any Derivative Works to the source code released from escrow that are made by or on behalf of the State shall be the sole property of the State. The State acknowledges that its ownership rights are limited solely to the Derivative Works and do not include any ownership rights in the underlying source code.

Glossary

Days	Means calendar days unless otherwise specified.
24x7x365	Means 24 hours a day, seven days a week, and 365 days a year (including the 366th day in a leap year).
Additional Service	Means any Services/Deliverables within the scope of the Contract, but not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
Audit Period	See Section 2.110
Business Day	Whether capitalized or not, shall mean any day other than a Saturday, Sunday or State-recognized legal holiday (as identified in the Collective Bargaining Agreement for State employees) from 8:00am EST through 5:00pm EST unless otherwise stated.
Blanket Purchase Order	An alternate term for Contract as used in the States computer system.
Business Critical	Any function identified in any Statement of Work as Business Critical.
Chronic Failure	Defined in any applicable Service Level Agreements.
Deliverable	Physical goods and/or commodities as required or identified by a Statement of Work
DTMB	Michigan Department of Technology, Management and Budget
Environmentally preferable products	A product or service that has a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. Such products or services may include, but are not limited to, those that contain recycled content, minimize waste, conserve energy or water, and reduce the amount of toxics either disposed of or consumed.
Excusable Failure	See Section 2.244.
Hazardous material	Any material defined as hazardous under the latest version of federal Emergency Planning and Community Right-to-Know Act of 1986 (including revisions adopted during the term of the Contract).
Incident	Any interruption in Services.
ITB	A generic term used to describe an Invitation to Bid. The ITB serves as the document for transmitting the RFP to potential bidders
Key Personnel	Any Personnel designated in Article 1 as Key Personnel.
New Work	Any Services/Deliverables outside the scope of the Contract and not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
Ozone-depleting substance	Any substance the Environmental Protection Agency designates in 40 CFR part 82 as: (1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or (2) Class II, including, but not limited to, hydro chlorofluorocarbons
Post-Consumer Waste	Any product generated by a business or consumer which has served its intended end use, and which has been separated or diverted from solid waste for the purpose of recycling into a usable commodity or product, and which does not include post-industrial waste.
Post-Industrial Waste	Industrial by-products that would otherwise go to disposal and wastes generated after completion of a manufacturing process, but do not include internally generated scrap commonly returned to industrial or manufacturing processes.
Recycling	The series of activities by which materials that are no longer useful to the generator are collected, sorted, processed, and converted into raw materials and used in the production of new products. This definition excludes the use of these materials as a fuel substitute or for energy production.
Reuse	Using a product or component of municipal solid waste in its original form more than once.
RFP	Request for Proposal designed to solicit proposals for services
Services	Any function performed for the benefit of the State.

Source reduction	Any practice that reduces the amount of any hazardous substance, pollutant, or contaminant entering any waste stream or otherwise released into the environment prior to recycling, energy recovery, treatment, or disposal.
State Location	Any physical location where the State performs work. State Location may include state-owned, leased, or rented space.
Subcontractor	A company Contractor delegates performance of a portion of the Services to, but does not include independent contractors engaged by Contractor solely in a staff augmentation role.
Unauthorized Removal	Contractor's removal of Key Personnel without the prior written consent of the State.
Waste prevention	Source reduction and reuse, but not recycling.
Waste reduction and Pollution prevention	The practice of minimizing the generation of waste at the source and, when wastes cannot be prevented, utilizing environmentally sound on-site or off-site reuse and recycling. The term includes equipment or technology modifications, process or procedure modifications, product reformulation or redesign, and raw material substitutions. Waste treatment, control, management, and disposal are not considered pollution prevention, per the definitions under Part 143, Waste Minimization, of the Natural Resources and Environmental Protection Act (NREPA), 1994 PA 451, as amended.
Work in Progress	A Deliverable that has been partially prepared, but has not been presented to the State for Approval.
Work Product	Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Contractor as a result of an in furtherance of performing the services required by this Contract.

Attachment 1 – Service Level Agreement

PERPETUAL USE LICENSE, IMAGETREND HOSTED SOLUTION VERSION 3.0

This agreement exists for the purpose of creating an understanding between ImageTrend and CLIENT who elect to host the application on ImageTrend's servers. It is part of our guarantee for exceptional service levels for as long as the system annual support fee is contracted. The Licensed ImageTrend Hosted Solution Service Level Agreement guarantees your web application's availability, reliability and performance. This Service Level Agreement (SLA) applies to any site or application hosted on our network as contracted.

1. Hosting at the ImageTrend's Datacenter

ImageTrend's hosting environment provides **99.9% availability** and is comprised of state-of-the-art Blade Servers and SAN storage that are configured with the no single point of failure through software and infrastructure virtualization, blade enclosure redundancies and backup storage policies. Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN. Scheduled maintenance and upgrades do not apply to the system availability calculation and all CLIENTs are properly notified of such scheduled occurrences to minimize accessibility interruptions.

Hardware

ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
 - Microsoft SQL Server 2012
 - Microsoft Windows Server 2008
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Disk Space allocation and Bandwidth as contracted

Physical Facility

The ImageTrend hosting facility is located in downtown Minneapolis with every industry standard requirement for hosting not only being met, but exceeded. Requirements such as power supply and power conditioning, normal and peak bandwidth capacity, security and fail over locations are all part of an overall strategy to provide the most reliable hosting facility possible.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression

- Secured site access
- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity

ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.
- Daily Scheduled backup Success/Failure notification via cell-phone and email

2. Application and Hosting Support

ImageTrend provides ongoing support as contracted for their applications and hosting services, including infrastructure. This includes continued attention to product performance and general maintenance needed to ensure application availability. Support includes technical diagnosis and fixes of technology issues involving ImageTrend software. ImageTrend has a broad range of technical support services available in the areas of:

- Web Application Hosting and Support
- Subject Matter Expert Application Usage Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

ImageTrend offers multi-level technical support, based on level-two user support by accommodating both the general inquiries of the administrators and those of the system users. We will give the administrators the ability to field support for the system as the first level of contact while providing them the option to refer inquiries directly to ImageTrend.

ImageTrend's Support Team is available 24/7 at support@imagetrend.com and www.imagetrend.com/support as well as Monday through Friday from 8:00 am to 5:30 pm CST at:

Toll Free: 1-888-730-3255
Phone: 952-469-1589

Online Support Desk

ImageTrend offers an online support system, Support Desk, which incorporates around-the-clock incident reporting of all submitted tickets to ImageTrend's support desk specialists. Once a client submits a support ticket, he or she can easily track its process with a secure login, promoting a support log for the client and ImageTrend's support team. The system promotes speedy resolution by offering keyword-based self-help services and articles in the knowledgebase, should clients wish to bypass traditional support services. Ticket tracking further enhances the efforts of Support Desk personnel by allowing them to identify patterns which can then be utilized for improvements in production, documentation, education and frequently asked questions to populate the knowledgebase. The support ticket tracking system ensures efficient workflow for the

support desk specialists while keeping users informed of their incident’s status. Support patterns can be referenced to populate additional knowledgebase articles.

Incident Reporting Malfunctions

ImageTrend takes all efforts to correct malfunctions that are documented and reported by the Client. ImageTrend acknowledges receipt of a malfunction report from a Client and acknowledges the disposition and possible resolution thereof according to the chart below.

Severity Level	Examples of each Severity Level:	Notification Acknowledgement: ImageTrend Return Call to Licensee after initial notification of an Error	Action Expectation: Anticipated Error resolution notification after ImageTrend Return Call to Licensee of Notification Acknowledgement of an error.
Severity 1 – Critical	<ul style="list-style-type: none"> - Complete shutdown or partial shutdown of one or more Software functions - Access to one or more Software functions not available - Major subset of Software application impacted 	Within one (1) hour of initial notification during business hours or via support@imagetrend.com or Support Desk with critical subject status.	Six hours
Severity 2 – Non-Critical	<ul style="list-style-type: none"> - Minor subsystem failure -Data entry or access impaired on a limited basis – usually can be delegated to local client contact as a first level or response for resolution – usually user error (i.e. training) or forgotten passwords 	Within four (4) hours of initial notification	24 Business hours
Severity 3 – Non-essential	<ul style="list-style-type: none"> - System operational with minor issues; suggested enhancements as mutually agreed upon – typically covered in next version release as mutually agreed upon. 	Same day or next business day of initial notification	Next Release

Service Requests (enhancements)

Any service requests that are deemed to be product enhancements are detailed and presented to the development staff, where the assessment is made as to whether these should be added to the future product releases and with a priority rating. If an enhancement request is specific to one client and deemed to be outside of the original scope of the product, then a change order is written and presented to the Client. These requests are subject to our standard rates and mutual agreement. Clients review and approve the scope, specification and cost before work is started to ensure goals are properly communicated.

Product release management is handled by ImageTrend using standard development tools and methodologies. Work items including, tasks, issues, and scenarios are all captured within the system. Releases are based on one or more iterations during a schedule development phase. This includes by not limited to: development, architecture, testing, documentation, builds, test and uses cases. Submissions of issues or requests are documented within our Product Management system and from there workflow is created to track the path from initial request to resolution.

Out of Scope

Client may contract with ImageTrend for Out of Scope services. This will require a separate Statement of Work and will be billed at ImageTrend's standard hourly rate.

Maintenance and Upgrades

System/product maintenance and upgrades, if applicable, are included in the ongoing support and warranty as contracted. These ensure continued attention to product performance and general maintenance. Scheduled product upgrades include enhancements and minor and major product changes. Customers are notified in advance of scheduled maintenance. It is the Client's responsibility to accept all offered updates and upgrades to the system. If the Client does not accept these, Client should be advised that ImageTrend, at its discretion, may offer limited support for previous versions. All code releases also maintain the integrity of any client specific configurations (i.e. templates, addresses, staff information, active protocols, etc.) that have been implemented either by ImageTrend's implementation staff or the client's administrative staff.

Escalation

Our support staff is committed to resolving your issues as fast as possible. If they cannot resolve your issue immediately, they will identify the course of action that they will be taking and indicate when an answer will be available. They in turn will seek assistance from the designated developer. The next level of escalation goes to the Project Manager, who also addresses all operational issues on an ongoing basis and reviews the issue log regularly to assess product performance and service levels. Senior Management will handle issues requiring further discussion and resolution. Any issues to be determined to be of a critical nature are immediately brought to the attention of both the X-Team and Senior Management.

Attachment 2 – Hosting Environment

Web/Application Server

Dual Quad Core Processors
32 GB RAM
SAN Data Storage
Blade Servers with Microsoft Hyper-V

Operating Systems

Microsoft Windows 2008 R2 Server

Web Server Software

Microsoft IIS version 7.0 or later

Addition Service Software

Microsoft .NET Framework 2.0, 3.5 SP1 and 4.0
Microsoft Tablet PC SDK

Additional Application Software

Adobe ColdFusion 9 Enterprise

Database Server (Separate database servers)

Hardware

Dual Quad Core Processors
8-16 GB RAM
100 GB Available Hard Disk Space
100,000 + incidents per year: 200 GB
RAID 5 SCSI Hard Drives

Software (64-bit recommended)

Microsoft SQL Server 2012

Internet Browser Requirements for End Users

Microsoft Internet Explorer 8.0 and above
Other browsers that support Mozilla 4.0 and above
Adobe Reader 10 or higher
Adobe Flash 11 or higher (recommended)
Microsoft Silverlight 2.0 (recommended)

Minimum Requirements for End Users using the DRF (Dynamic Run Form)

Software

Microsoft Silverlight 3.0

Hardware

OS: Windows XP SP2
RAM: 1GB
Processor: 1.2 GHz

Network

64 kbps ISDN/DSL (Cable or DSL)

ImageTrend Hosting

Integral to any online solution is a quality data center providing application access, availability, data security and overall confidence. ImageTrend's facilities incorporate industry leading infrastructure, application security and excellent technical support for our hosted solutions. ImageTrend offers experience and the latest technology for our hosted applications. To date over 60,000,000 incidents have been documented and stored utilizing ImageTrend Bridge products. Another benefit to an ImageTrend hosted solution is the long-term cost savings to the client in hardware investments and maintenance and the staff levels and commitment to maintaining a datacenter that is secure and reliable for HIPAA data storage.

System Upgrades/Updates

As a system hosted by ImageTrend, we manage all aspects of the software installation and server infrastructure. Any upgrades are applied following a release schedule, which includes prior notification of the availability of the upgrade, the anticipated scheduled maintenance and allowing for sufficient time to accommodate any client concerns or constraints. Our virtual infrastructure supports many types of upgrades or fixes to be applied without any system downtime and therefore unnoticed by a client. Updates to the Field Bridge are administrated through the Service Bridge. The system administrator can determine when to push the updates to the Field Bridge. The update is then installed by Windows restricted users. The Field Bridge user will get a message at login indicating that an update is available. They can choose to install or cancel. The user does not have to be an administrator to run an update.

If the application is hosted by the client, our staff notifies the client's staff that an upgrade is available with recommendations for installation. We may assist in this provided we are given a VPN and system access.

License Options

Over 70% of ImageTrend's solutions are hosted at ImageTrend's data center. Any of those solutions hosted with ImageTrend may have the solution's licensure offered as a one-time purchase or it can be included in the monthly hosting fees, which ImageTrend defines as Software as a Service (SaaS) – application usage lease, support and hosting in one annual fee. All solutions provided by ImageTrend can alternatively be hosted at the client's data center.

Availability

ImageTrend's hosting environment provides 99.9% availability and is comprised of state-of-the-art Blade Servers and SAN storage that ensure this with software and infrastructure virtualizations, blade computing redundancies and backup storage policies. Our data center service is recognized by Microsoft as being in the top 100 of their "Top Tiered Hosting Partners". If 99.99% availability is desired, which includes our second data center in Chicago, additional hosting costs will apply.

Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN.

Data Retention

Information will be stored in the system for as long as desired by the client. Archived information will still be accessible by the System Administrators. Data will only be purged upon a client request.

Hardware

ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
 - Microsoft SQL Server 2012
 - Microsoft Windows Server 2008 R2
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Weekly, monthly or quarterly backups (as contracted)
- Periodic CD-ROM backups (as contracted)
 - Weekly, monthly or quarterly
 - Offsite vaulting and escrow
- 30 GB Disk Space allocation per month with additional space in 10 GB increments
- 3 Mb Traffic or Bandwidth per month with additional bandwidth available in 1 Mb increments

Physical Facility

The ImageTrend hosting facility is located in downtown Minneapolis with every industry standard requirement for hosting not only being met, but exceeded. Requirements such as power supply and power conditioning, normal and peak bandwidth capacity, security and fail over locations are all part of an overall strategy to provide the most reliable hosting facility possible.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression
- Secured site access
- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity

ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.

- Daily Scheduled backup Success/Failure notification via cell-phone and email

Support Services

ImageTrend provides both onsite and on-call support for their applications and hosting. Support includes technical diagnosis and fixes of technology issues involving software and hardware. ImageTrend has a broad range of technical support to their systems and proposes to provide service in the areas of:

- Web Site Hosting and Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

Phone support is available Monday through Friday from 7:00 AM - 6:00 PM CST. ImageTrend also provides onsite resolution for support of their applications either at their location in Lakeville, MN or at the client's location as the situation dictates.

Attachment 3 – ImageTrend Security and Disaster Recovery Process

ImageTrend has included information describing the security for the IT environment in this section of our response, as well as our Disaster Recovery Plan. The EDS Data Security Policies and Procedures document has been included in Attachment 4.

Security

ImageTrend applications meet or exceed State and federal data privacy requirements and the HIPAA guidelines. Secure logins are an industry standard process and are part of the HIPAA guidelines for data protection. These are implemented throughout the application with the use of the hierarchical security access features of the ImageTrend security module, which provides the environment for controlling the access necessary to provide data protection. The application also provides for security breach notifications and audit trails.

Application Securities

Secure User Login

- The application adheres to business standard practices for security to ensure only authorized access to the system

Password Encryption

- Hash function implementation
- Temporary account suspension for sessions failing to successfully login after three tries
- Check access log for sequential unsuccessful logins
- Set session logout variable

Password Requirements

- Length and Complexity Enforcement
- Validate Password for Case, Length (8 characters), and Composition

Login Expirations

- Validate for expired logins
- Force password changes on expired logins and restrict site access until new, valid password is created

Page Access Checking

- Page Access Checking to make sure user has properly logged in and is not entering the site via an external link

SSL Server Certificate

- 128-bit encryption Security Certificate

Permissions Administration

Manage Users and Groups

The application employs a hierarchical based password administration as a series of group policies to control application entry and level of access within the application. With the system administrator being the highest level of security, groups can be created below that to encompass all other group needs, which may include:

- Director – Access to view all runs within their service.
- Multiple Service Administrators – User Access and administration to multiple services.

Permissions and Rights

Permission and rights are governed by the ability of what the user can see and do. At the global level, rights are based on the following criteria:

- County
- City
- Service

On the service level, there are two levels:

- Administrator
- User

Service administrators can control and edit all the functions with their own service. Service users have the ability to edit and view their own information.

Password Administration

Through the Application Access Control, the system administrator can determine several features regarding the password administration:

- Number of days without login to the application before the user's account is suspended
- Number of attempts a user can attempt to login before their account is placed on temporary suspend
- Set the password to contain at least one numeric character
- Set the password to contain at least one uppercase character
- Time in hours that a user cannot change their password after last change
- Number of past passwords stored in the log table for a user
- Number of passwords in the log table to be compared with the newest password to prevent repeat use of passwords
- Minimum number of characters in the password
- Number of days the user will be notified before they must change their password
- An Email Confidentiality statement can be added, edited and deleted
- An inactive account message can be added, edited and deleted
- Security questions prompt on login or password retrieval
- Encrypt security question answer

Procedural Securities

Hosting Environment

ImageTrend's Web applications are hosted in our state-of-the-art, 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically and a log book is kept to monitor and record individuals accessing the server room.

ImageTrend's production network consists of application/web and database servers. The databases are on a private network with access control managed through the firewall, permitting only authorized administrators or approved VPN access.

Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation trigger email alerts which are sent to support staff and cell phone alerts to ImageTrend's 24/7 X-Team Support staff. Our X-Team support employees have VPN access to our production servers, to ensure accessibility and security, when accessing our servers from outside of our network

Auditing

The Service Bridge's audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database. This database is kept for a period of time for reporting purposes and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosures. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

Personnel

All ImageTrend employees are subjected to background checks and are required to attend and successfully complete HIPAA training. The ImageTrend Project Management System gives us a facility to track any HIPAA Security Incidents or Information Disclosure Incidents for reporting purposes.

Only those certified ImageTrend employees that work with either hardware or software related to the specified application or project will access the data center and interact with our servers. These employees have worked with our hardware as part of our IT support staff or are part of our Implementation team as software developers. Authorization is granted from the management level.

Disaster Recovery

ImageTrend, Inc. follows a specific critical path for organizations and companies during a recovery effort, to ensure the resumption of normal operations in the event of a disaster. This process has seven stages, which are followed regardless of the organization. In a disaster recovery plan it is important to minimize the loss of data and return application usage as quickly as possible.

Stage 1 - Immediate Response

The first step in the recovery process and the initial reaction to a potential disaster or interruption consists of immediate assessment and if necessary, notification of clients of interruption and any actions they should undertake. In many situations the system's redundancies will accommodate the situation and provide continuity. This takes place within the first 4 hours.

Stage 2 - Environment Restoration

The necessary steps for restoring service via repairs or alternate infrastructure are begun by gathering the necessary components for restoration and installing. If local repair is not possible due to extreme conditions, then the service will be redirected to another data center and the required DNS redirection may take up to 8 hours to propagate.

Stage 3 - Functional Restoration

Application functionality is tested on restored or alternate service site to ensure user access and usability. For same data center restoration within 8 hours and for alternate site usage within 24 hours.

Stage 4 - Data Restoration and Synchronization

This step includes backlog reduction. Data from offsite locations is restored to the restored environment. Database backups are automatically done every 2 hours, daily and weekly. These backups will be used for data restoration and synchronization. Maximum data window will be two hours. Most often, data is protected at different times during the business cycle and must be reconstructed or synchronized before it can be used. Synchronizing, validating, and reviewing data from many different sources is a critical step in a successful recovery. Once reliable data is established, backlogged transactions that have accumulated during recovery can be processed. This may take up to 48 hours, however application usage is available during this time.

Stage 5 - Business Resumption

Clients will be notified that the affected service can now resume its normal operations.

Stage 6 - Interim Site Migration

Once the primary site environment has been restored, return migration is planned and scheduled. Depending on the nature of the problem, this may take an extended period of time to restore the environment. Disruption of services during this transition will be minimized and clients will be notified of the impact and a schedule of return will be mutually discussed.

Stage 7 - Return to Home Site

All recovery efforts have been completed, and a business may resume normal operations at its primary location.

Backups

Code Backups

Application code is backed up daily; at least a daily backup exists for all applications hosted in ImageTrend's production environment and is included in hosting costs. These backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. Daily backups are retained for longer as unallocated storage permits but not guaranteed to be available beyond the previous calendar day. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Database Backups

Database files are backed up daily; at least a daily backup exists for any database hosted in ImageTrend's production environment and is included in hosting costs. Daily backups are retained for several days as unallocated storage permits but not guaranteed to be available beyond three previous calendar days. Database backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Restore Procedures

Daily backup files are stored uncompressed to facilitate quick recovery of one or more files as needed. Archive copies are compressed to conserve disk space. All database files are compressed to conserve disk space and must be uncompressed and reattached for restoration. When restoring a file the newer file, if it exists, is renamed and kept before replacing with the backup version. When restoring an entire database file, the copy being replaced is itself backup up before being modified. When restoring part of a database file, the current file is first backed up and the backup database is mounted with a different name, then the needed tables are restored and the backup file is detached. If restoring a complete backup of application code over a corrupted install, a copy of the bad files is kept to maintain any new user-added files since the backup was created.

Attachment 4 – EDS Data Security Policies and Procedures

DATA SECURITY POLICY OVERVIEW

This document defines the data security policy of ImageTrend, Inc. ImageTrend, Inc. takes the privacy of our employees and clients very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.

Intent

The goal of this policy is to inform ImageTrend employees and customers of the rules and procedures relating to data security compliance.

The ImageTrend data covered by this policy includes, but is not limited to all electronic information found in e-mail, databases, applications and other media; paper information, such as hard copies of electronic data, employee files, internal memos, and so on.

The Client data covered by this policy includes, but is not limited to all electronic information collected by any ImageTrend software application, which is hosted at the ImageTrend data center.

Audience

This policy applies to all employees, management, contractors, vendors, business partners and any other parties who have access to company and/or client data.

Data Types

ImageTrend, Inc. deals with two main kinds of data:

1. **Company-owned data** that relates to such areas as corporate financials, employment records, payroll, etc.
2. **Private data** that is the property of our clients and/or employees, such as social security numbers, credit card information, contact information, patient data, etc.

Data Classifications

ImageTrend, Inc.'s data is comprised of 3 classifications of information:

1. **Public/Unclassified.** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials, and other data as applicable.

Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. **Private.** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies, and other data as applicable.

All information not otherwise classified will be assumed to be Private.

Employees may not disclose private data to anyone who is not a current employee of the company.

3. **Confidential.** This is defined as personal or corporate information that may be

considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as

applicable]. ImageTrend, Inc. considers it a top priority to protect the privacy of our clients and employees

Employees may only share confidential data within the department or named distribution list and with proper authorization.

4. **Secret/Restricted.** This is defined as sensitive data which, if leaked, would be harmful to ImageTrend, Inc., its employees, contractors, and clients. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes but is not limited to audit reports, legal documentation, business strategy details, patient data, and other data as applicable.

Secret/restricted data cannot be disclosed by anyone other than the original author, owner or distributor.

It is the responsibility of everyone who works at ImageTrend, Inc. to protect our own and client data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

Responsibilities

All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.

Management is responsible for ensuring that their direct reports understand the scope and implications of this policy. HR must also ensure that all employees attend data privacy training and have evidence thereof and a signed copy of this policy in their file.

Security staff will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.

Any employee who authors or generates corporate or client data must classify that data according to the criteria outlined above.

Management

Ownership of this policy falls to Security Officer. For any questions about this policy, or to report misuse of corporate or personal data, please contact him/her at (952) 469-1589. The IT department will work in conjunction with the client to maintain data access privileges, which will be updated as required when an employee joins or leaves the company. These are the accepted technologies ImageTrend, Inc. used to enforce and ensure data security:

1. Access controls
2. Strong passwords
3. System monitoring
4. Personnel Training

Review

Management is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

On an annual basis, unless previous action was required, we review our security policies and procedures to ensure that necessary updates have occurred. We welcome any security reviews that our customers might request at their expense. Several clients have performed such reviews over the years and have been satisfied with the results.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPLICATION SECURITY

DATA WAREHOUSE SECURITY

EMS State Bridge/EMS Service Bridge/Rescue Bridge

The ImageTrend applications meet or exceed State and federal data privacy requirements and the HIPAA guidelines. Secure logins are an industry standard process and are part of the HIPAA guidelines for data protection. These are implemented throughout the application with the use of the multi-tiered hierarchical security access features of the ImageTrend security module, which provides the environment for controlling the access necessary to provide data protection.

The reporting and auditing functions of the application's procedures allow for safeguarding and immediate notifications of any attempted breaches. This provides for data access only through assigned permissions and ensures that only those intended see their data and can access it for reporting.

Application Securities

- Secure User Login
- Password Encryption
- Password Requirements
- Login Expirations
- Page Access Checking
- SSL Server Certificate: 128-bit encryption Security Certificate
- CAD data sent using secure Web Service

Permissions Administration

Manage Users and Groups

The application employs a hierarchical based password administration as a series of group policies to control application entry and level of access within the application. With the system administrator being the highest level of security, groups can be created below that to encompass all other group needs, which may include:

- Director – Access to view all runs within their service.
- Multiple Service Administrators – User Access and administration to multiple services.

Permissions and Rights

Permission and rights are governed by the ability of what the user can see and do. At the global level, rights are based on the following criteria:

- County
- City
- Service

On the service level, there are two levels:

- Administrator
- User

Service administrators can control and edit all the functions with their own service. Service users have the ability to edit and view their own information.

Password Administration

Through the Application Access Control, the system administrator can determine several features regarding the password administration:

- Number of days without login to the application before the user's account is suspended
- Number of attempts a user can attempt to login before their account is placed on temporary suspend
- Set the password to contain at least one numeric character
- Set the pass word to contain at least one uppercase character
- Number of past passwords stored in the log table for a user
- Number of passwords in the log table to be compared with the newest password to prevent repeat use of passwords
- Minimum number of characters in the password
- Number of days the user will be notified before they must change their password
- An Email Confidentiality statement can be added, edited and deleted
- An inactive account message can be added, edited and deleted
- Security questions prompt on login or password retrieval
- Encrypt security question answer

Procedural Securities

Hosting Environment

ImageTrend's Web applications are hosted in our state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book is kept to monitor and record individuals accessing the server room.

ImageTrend's production network consists of application/web and database servers. The databases are on a private network with access control managed through the firewall permitting only authorized administrators or approved VPN access.

Applications are monitored for availability and performance from multiple locations to ensure an accurate measure of current system health. Slow application pages and long running database queries are logged for analysis by server administrators and development staff. Serious errors and performance degradation trigger email alerts which are sent to support staff and cell phone alerts to ImageTrend's 24/7 X-Team Support staff. Our X-Team support employees have VPN access to our production servers, to ensure accessibility and security, when accessing our servers from outside of our network.

Auditing

The system's audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database, which is kept for a period of time for reporting purpose and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosers. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

FIELD COLLECTION SECURITY

EMS Field Bridge

Security for Field Bridge conforms to the current best practices and new technology. Security enhancements have been performed both behind the scenes with increased database security and through settings that administrators can configure for automatic run removal and password requirements.

Data Storage Security

Data storage for each Field Bridge works with Microsoft SQL CE 2008. This software provides greater data security for all patient data. The databases contained within SQL CE 2008 are password protected to prevent unauthorized access and the entire database is completely encrypted with 128-bit encryption. In addition, all patient data within the database is further encrypted using Rijndael (AES) cipher algorithm using a 128-bit key and IV, assemblies are obfuscated and string encrypted. Data received through a CAD integration is sent via secure Web Services.

Data Sync to Service/Rescue/State Bridge

The ImageTrend EMS Field Bridge complies with W3C web Service and XML standards. Data is synced from the Field Bridge to the Service/Rescue/State Bridge through secure web service communication utilizing 128-bit SSL Certificate which encrypts all data during transmission.

There are three authentication parameters that are required to be sent with the web service request as outlined below. A user account will be set up within the Field Bridge system to track access and assign any actions to a particular user. An additional API token will be created for web service authentication.

- token=uniqueidentifier
- userID=string
- password=string

Administrative-Set Security Options

Administrators have the ability to configure the Field Bridge to provide additional security. Additional security is possible based on your service's IT departments and policies.

Clearing Out Old Incidents

Administrators can choose to delete old incidents from the Field Bridge database after a certain number of days and after those incident reports have been posted to the Service Bridge, State Bridge or Rescue Bridge system working with this Field Bridge. Automatically removing old incidents will reduce the amount of patient data available in the system at any one time without causing any additional time to manually clean out the database, reducing any risk of a security issue.

Usernames and Passwords

Within the Field Bridge, any user who wants to work with the application must log in with a username and password set up on the Service Bridge, State Bridge or Rescue Bridge to which this Field Bridge is assigned. Administrators can set up the password requirements, the length of time in between required password changes and any restrictions on the user's access to portions of the Field Bridge.

HOSTING OVERVIEW

ImageTrend's hosting environment provides 99.9% availability and is comprised of state-of-the-art Blade Servers and SAN storage that ensure this with software and infrastructure virtualizations, blade computing redundancies and backup storage policies. Our data center service is recognized by Microsoft as being in the top 100 of their "Top Tiered Hosting Partners".

Our Compellent SAN has a fiber channel backend, currently hosts 8TB of storage, has dual storage controllers with redundant power supplies and redundant paths to disk, and hot swappable drives. We do offsite replication to disk on a second SAN. Information will be stored in the system for as long as desired by the client. Archived information will still be accessible by the System Administrators. Data will only be purged upon a client request.

Hardware

ImageTrend server hardware is configured to prevent data loss due to hardware failure and utilize the following to ensure a quick recovery from any hardware related problems.

- Independent Application and Database Servers
 - Microsoft SQL Server 2012
 - Microsoft Windows Server 2008
- Redundant Power Supplies
- Off-Site Idle Emergency Backup Servers (optional)
- Sonicwall VPN Firewall
- Redundant Disk configuration
- Weekly, monthly or quarterly backups (as contracted)
- Periodic CD-ROM backups (as contracted)
 - Weekly, monthly or quarterly
 - Offsite vaulting and escrow
- 30 GB Disk Space allocation per month with additional space in 10 GB increments
- 3 Mb Traffic or Bandwidth per month with additional bandwidth available in 1 Mb increments

Physical Facility

ImageTrend's Web applications are hosted in our state-of-the-art 4,500 square foot data center. Built in a vault with 21" concrete walls, our facilities offer the maximum level of security and stability for hosting needs. The data center features triple redundant, high-speed internet connections over fiber optic trunk lines. Only authorized personnel have access to the data floor. The data center is monitored electronically, as well as a log book is kept to monitor and record individuals accessing the server room.

- Redundant, high-speed Internet connections over fiber optics.
- Power protection via an in-line 80kVa UPS with a 150 KW backup diesel generator
- Temperature controlled
- Waterless Fire Protection and Clean agent fire suppression
- Secured site access
- Steel Vault Doors
- 21" concrete walls and ceiling

Data Integrity

ImageTrend applications are backed up daily allowing for complete recovery of data to the most recent backup:

- Daily Scheduled Database and Application Backups.
- Daily Scheduled backup Success/Failure notification via cell-phone and email

SERVER MONITORING

This section outlines the process followed to ensure server stability and proactively reduce server incidents.

Server Status

All ImageTrend production servers are monitored 24/7 for system health and service availability. Status information includes:

- current users accessing the system
- disk use
- memory use
- CPU use
- Notification of hardware failures

Server logs are kept on a separate server and are available for review even in the event that a server fails for forensic use in determining the state shortly before a problem occurred. Server status is recorded and any dramatic change in a metric generates an alert message to all available support staff.

Application Status

All ImageTrend production servers are monitored 24/7 for the status of Web services and ImageTrend applications. Status information includes:

- application availability
- application response time
- failure status codes

A change in application status generates an alert message to all available support staff. General application responsiveness is tested, not individual client sites are monitored, so an error in a single application may go undetected by this system.

Monitoring Intervals and Response Times

Monitoring events occur between every three and eight minutes depending on the application and server being monitored. Monitoring takes place from multiple locations with staggered start times resulting in a monitoring resolution of approximately two to five minutes. Alerts generated by the monitoring system are sent to support staff via email and SMS to cell phones, with an average transmission time of one minute.

SERVER INCIDENT RESPONSE

Service Recycling

The most common cause of service unavailability is a failed service. A failed service is given 10 minutes to recycle or the problem is escalated to a server restart. Other action may be taken as the situation warrants, given service specific errors or an obvious cause for the failure.

Server Restart

A server restart should be undertaken if a service recycling does not solve the failure or further troubleshooting. Normal operating system functions for restarting should be used if possible. Otherwise using ImageTrend's remote controllable power outlets the server should be cold booted. The progress of the restart is observed using ImageTrend's IP enable KVM switch allowing BIOS or other hardware errors to be observed and worked through.

Transferring Websites

If within 50 minutes of the initial alert being issued services have not been restored and a solution does not appear to be immediately forthcoming, the services and roles of the unavailable server will be moved to an alternate location. ImageTrend maintains an extra server capacity to allow for this flexibility with minimal disruption to other services. If the original files are unavailable backups will be used to recreate the original server configuration. As the same IP addresses are used to restore service no DNS changes are required and the restoration is immediate. While in transition the websites affected will display a message describing the problem and an estimation of the time to service being restored.

Transferring Locations

If service cannot be restored by transferring to a different server within the same environment, services will be moved to an alternate hosting location. A backup datacenter is available in Chicago, IL, for hosting mission critical applications. Code and database backups are pushed to this location to be used in the event of disaster which disables the primary datacenter in Minneapolis, MN. Clients requiring automatic failover can opt for DNS failover which detects service unavailability and automatically moves DNS records to refer to the backup location. Other clients will be moved to the backup datacenter as needed and DNS changes will be made manually or requested immediately upon the initiation of relocation.

Hardware Replacement

Whenever a hardware failure contributes to a server failure the hardware in question will be replaced aggressively before redeploying the system. For instance, a failed drive will be replaced; multiple drive failure will require all drives be replaced as well the power supply and possibly drive cables if damage is evident. If a system operates for an extended period without cooling fans the system components will be retired from production use and completely replaced.

AUDIT FUNCTIONALITY

Our site monitor audit trail tracks user information when accessing the secure portion of the application. IP address, User ID, date/time, browser information, along with information on each file accessed, is all tracked within a separate database, which is kept for a period of time for reporting purposes and audit trails.

Any security breaches are logged within our Project Management system for any HIPAA disclosures related to security breaches or information disclosures. If a security breach happens, the security module currently sends an email to our Director of Development and the Security Officer, who in turn notifies the designated customer contact.

There are also numerous reports for data import to track user, date/time, import type, number of records, validity, and total import time.

Audit Reports Available

- Audit Report
- Validity Audit Report
- Field Audit Report
- Run Report
- Run Variance Report

When run incidents enter the system, they are tracked on both date and time and the user that entered that run. It will also track the date/time that a user that last updated that information. In addition to the audit trail, there are addendum and attachment features within the system. Addendums allow staff to enter additional text to track changes within an existing run report, or attach any necessary files.

A history trail for each run report tracks staff usage including date/time and user for:

- Generating PDF Run Reports
- Adding addendums
- Changing run status
- Changing run lock status
- Adding attachments
- Viewing repeat patient

SYSTEM BACKUPS

ImageTrend provide backup coverage for continuity purposes as well as data archive purposes. Define backup and retention policies to clearly establish expectations of coverage. Define continuity resources and locations. Meet or exceed contract and other obligations.

Code Backups

Application code is backed up daily; at least a daily backup exists for all applications hosted in ImageTrend's production environment and is included in hosting costs. These backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. Daily backups are retained for longer as unallocated storage permits but not guaranteed to be available beyond the previous calendar day. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Database Backups

Database files are backed up daily; at least a daily backup exists for any database hosted in ImageTrend's production environment and is included in hosting costs. Daily backups are retained for several days as unallocated storage permits but not guaranteed to be available beyond three previous calendar days. Database backups are retained for particular customers as needed on a weekly, monthly, quarterly or annual basis as agreed to by contract. All backup routines execute after peak hours to minimize the effect on users, typically between 11 PM and 4 AM Central Time. Backups are stored on hard disks, with a copy being taken offsite on a monthly basis, and tape cassettes which are rotated on a daily basis. Data synchronization is run across a secure network connection back to ImageTrend's offices in Lakeville, MN, on an irregular basis for both application code and database files.

Restore Procedures

Daily backup files are stored uncompressed to facilitate quick recovery of one or more files as needed. Archive copies are compressed to conserve disk space. All database files are compressed to conserve disk space and must be uncompressed and reattached for restoration. When restoring a file the newer file, if it exists, is renamed and kept before replacing with the backup version. When restoring an entire database file, the copy being replaced is itself backed up before being modified. When restoring part of a database file, the current file is first backed up and the backup database is mounted with a different name, then the needed tables are restored and the backup file is detached. If restoring a complete backup of application code over a corrupted install, a copy of the bad files is kept to maintain any new user-added files since the backup was created.

Backup Goals

ImageTrend has several goals for our backup coverage:

- Provide simple and rapid continuity resources
- Provide adequate backup coverage to meet contract and other obligations
- Substitute redundant active resources for continuity backups where reasonable
- Clearly define specific backup policies which differ from the standards
- Maintain a backup window with minimal impact on performance and availability

Minimal Backup Contents

Backups for all data must include:

- One copy of current application files, updated nightly and stored on separate disks from those hosting the application

- One copy of current database files, updated nightly and stored on separate disks from those hosting the database
- One copy of current system configurations, updated nightly and stored on separate disks from those hosting the system
- Alternate retention policies for a specific application must be laid out in writing, specifying requirements for frequency of backups, retention period and coverage requirements

Archive Backup by category

Standard

- No archive required (0)
- Week of daily archives recommended (8)
- Archives- Minimum: 0, Recommended: 8

Important

- Two weeks of daily archives required (15)
- One month of weekly archives required (4)
- Six months of monthly archives required (6)
- Two months of weekly and 1 year of monthly archives recommended (8,12)
- Archives- Minimum: 25, Recommended: 34

Critical

- Four weeks of daily archives required (29)
- Three months of weekly archives required (12)
- 1 year of monthly archives required (12)
- 1 year of weekly archives recommended (52)
- Archives- Minimum: 53, Recommended: 76

Optional

- No continuity or archives required
- Single continuity backup recommended
- Archives- Minimum: 0, Recommended: 1

Continuity Backup by category

Standard

- Continuity restoration within hours

Important

- Continuity restoration within one hour

Critical

- Continuity restoration within 30 minutes

Optional

- No continuity or archives required

Offsite backup by category

All offsite backups are stored encrypted on disk in a locked fire cabinet in ImageTrend's offices or replicated to other collocation sites per the following categories.

Standard

- Monthly offsite backup is stored

Important

- Monthly offsite backup is stored, offsite replication may be performed per availability requirements

Critical

- Monthly offsite backup is stored, offsite replication may be performed per availability requirements

Optional

- Optical disc based or electronic transmission backups sent to clients may be performed on a negotiated schedule

Terms

Continuity Backup

Data Archive Backup

Full Backup

Incremental Backup

Differential Backup

Week of daily archives

Weekly archive

Monthly archive

Definitions

An exact and current as possible copy of all files, data and system configurations comprising an application

Stored backups for the purposes of restoring data to a specific point in the past

A complete copy of all data at that moment in time

A copy of all new or modified files since last full or incremental backup

A copy of all new or modified files since last full backup

previous week's full backup, this week's full backup and the past six day's nightly differential backups

Full backup made on single day of the week (e.g., Sunday morning)

Full backup made on single day of the month (i.e. the First of the month, or first Sunday of the month)

DISASTER RECOVERY

ImageTrend, Inc. follows a specific critical path for organizations and companies during a recovery effort, to ensure the resumption of normal operations in the event of a disaster. This process has seven stages, which are followed regardless of the organization.

ImageTrend' EMS solutions consist of EMS State Bridge and Field Bridge, hosted at our facilities. In a disaster recovery plan it is important to minimize the loss of data and return application usage as quickly as possible.

Stage 1 - Immediate Response

The first step in the recovery process and the initial reaction to a potential disaster or interruption consists of immediate assessment and if necessary, notification of clients of interruption and any actions they should undertake. In many situations the system's redundancies will accommodate the situation and provide continuity. This takes place within the first 4 hours.

Stage 2 - Environment Restoration

The necessary steps for restoring service via repairs or alternate infrastructure are begun by gathering the necessary components for restoration and installing. If local repair is not possible due to extreme conditions, then the service will be redirected to another data center and the required DNS redirection may take up to 8 hours to propagate.

Stage 3 - Functional Restoration

Application functionality is tested on restored or alternate service site to ensure user access and usability. For same data center restoration within 8 hours and for alternate site usage within 24 hours.

Stage 4 - Data Restoration and Synchronization

This step includes backlog reduction. Data from offsite locations is restored to the restored environment. Database backups are automatically done every 2 hours, daily and weekly. These backups will be used for data restoration and synchronization. Maximum data window will be two hours. Most often, data is protected at different times during the business cycle and must be reconstructed or synchronized before it can be used. Synchronizing, validating, and reviewing data from many different sources is a critical step in a successful recovery. Once reliable data is established, backlogged transactions that have accumulated during recovery can be processed. This may take up to 48 hours, however application usage is available during this time.

Stage 5 - Business Resumption

Clients will be notified that the affected service can now resume its normal operations.

Stage 6 - Interim Site Migration

Once the primary site environment has been restored, return migration is planned and scheduled. Depending on the nature of the problem, this may take an extended period of time to restore the environment. Disruption of services during this transition will be minimized and clients will be notified of the impact and a schedule of return will be mutually discussed.

Stage 7 - Return to Home Site

All recovery efforts have been completed, and a business may resume normal operations at its primary location.

TESTING PROCESSES

SOFTWARE SECURITY VULNERABILITY TESTING

ImageTrend understands the importance of data security and consistently addresses the latest advances in regulations and technologies to ensure that our systems and processes meet federal and state data security standards. Our application security is designed to OWASP best practices and our hosting infrastructure is the latest 3-tier firewall configuration. Application access utilizes 128 bit encrypted secure socket layers and data transfers are encrypted as well. Our QA includes the use of IBM AppScan, which provides:

- Static analysis security testing to identify vulnerabilities at the source
- Automated web application scanning and testing with intelligent fix recommendations
- Extended coverage through Glassbox analysis and JavaScript Security Analyzer
- Automated correlation of static and dynamic analysis results

Security reviews have been conducted by several individual government organizations prior to their purchase of our applications with satisfactory results.

ADA TESTING PROCESS

ImageTrend follows ADA WCAG 2.0 level conformance guidelines. Resources are created and designed using xml, css, mathml, SMIL, SVG and other open standards that have features to support accessibility by people with disabilities. The client-facing pages follow the standards set in the ADA WCAG 2.0 accessibility guidelines to level AA conformance. ImageTrend performs audits of its product's accessibility and works to improve its conformance through regularly scheduled product upgrades. As with all of its products, ImageTrend, Inc. extends an ongoing effort to conform application to Level AA – ADA Conformance for Web Content Guidelines. We offer all of our clients the opportunity to perform testing on our web based applications to determine compliance with their own policies, needs, and/or requests. Should these tests result in modification or enhancement requests, they will be reviewed as to applicability within our planned product roadmap or handled as client-specific requests.

INFORMATION SENSITIVITY POLICY

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of ImageTrend without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing).

All employees familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect ImageTrend Confidential information (e.g., ImageTrend Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager.

Data Privacy

ImageTrend respects and understands the need for data privacy and the methods and functions needed to ensure this for both ImageTrend data and Client data. Software application, data center infrastructure, policies and procedures all play an integral role in this. Our staff reviews all updates whether from our partners (Microsoft and Adobe), federal and state legal opinions and guidelines or standards organizations to ensure that we are continually informed of the latest requirements. Our designers and developers continually monitor best practices and technological advances to ensure data privacy. ImageTrend's data center is located in a bank vault and has all of the physical controls in place to ensure security. Our staff is trained in the needs and processes required for data privacy and are all subjected to background checks.

On an annual basis, unless previous action was required, we review our security policies and procedures to ensure that necessary updates have occurred. We welcome any security reviews that our customers might request at their expense. Several clients have performed such reviews over the years and have been satisfied with the results.

HIPAA Training

All ImageTrend employees are subjected to background checks and are required to attend and successfully complete HIPAA training. The ImageTrend Project Management System gives us a facility to track any HIPAA Security Incidents or Information Disclosure Incidents for reporting purposes.

Only those certified ImageTrend employees that work with either hardware or software related to the specified application or project will access the data center and interact with our servers. These employees have worked with our hardware as part of our IT support staff or are part of our Implementation team as software developers. Authorization is granted from the management level.

Scope

All ImageTrend information is categorized into two main classifications:

- ImageTrend Public
- ImageTrend Confidential

ImageTrend Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to ImageTrend Systems, Inc.

ImageTrend Confidential contains all other information. Confidential information is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Information that should be protected very closely includes trade secrets, development programs, potential acquisition targets and other information integral to the success of our company. Also included in ImageTrend Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of ImageTrend Confidential information is "ImageTrend Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to ImageTrend by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders and supplier information. Information in this category ranges from extremely sensitive to information about connecting a supplier/vendor into ImageTrend's network to support our operations.

ImageTrend personnel are encouraged to use common sense judgment in securing ImageTrend Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their manager.

Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as ImageTrend Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the ImageTrend Confidential information in question.

Minimal Sensitivity

Minimal sensitivity data includes general corporate information and some personnel and technical information.

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential."

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "ImageTrend Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "ImageTrend Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, ImageTrend information is presumed to be "ImageTrend Confidential" unless expressly determined to be ImageTrend Public information by an ImageTrend employee with authority to do so.

Guidelines for Minimal Security Data

- **Access.** Granted to ImageTrend employees, contractors, people with a business need to know.
- **Distribution within ImageTrend.** Allowed in standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Allowed with U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

- **Electronic distribution.** No restrictions except that it is sent to only approved recipients.
- **Storage.** Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- **Disposal/Destruction.** Deposit outdated paper information in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive

More sensitive data includes business, financial, technical and most personnel information

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential."

As the sensitivity level of the information increases, in addition to or instead of marking the information "ImageTrend Confidential" or "ImageTrend Proprietary," you may wish to label the information "ImageTrend Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Guidelines for More Sensitive Data

- **Access.** Granted to ImageTrend employees and non-employees with signed non-disclosure agreements who have a business need to know.
- **Distribution within ImageTrend.** Allowed with standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Can be sent via U.S. mail or approved private carriers.
- **Electronic distribution.** No restrictions on sending to approved recipients within ImageTrend, but should be encrypted or sent via a private link to approved recipients outside of ImageTrend premises.
- **Storage.** Individual access controls are highly recommended for electronic information.
- **Disposal/Destruction.** Allowed in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code and technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

To indicate that ImageTrend Confidential information is very sensitive, you may should label the information "ImageTrend Internal: Registered and Restricted", "ImageTrend Eyes Only," "ImageTrend Confidential" or similar labels at the discretion of your individual

business unit or department. Once again, this type of ImageTrend Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Guidelines for Most Sensitive Data

- **Access.** Granted to only those individuals (ImageTrend employees and non-employees) designated with approved access and signed non-disclosure agreements.
- **Distribution within ImageTrend.** Must be delivered direct — signature required, envelopes stamped confidential or approved electronic file transmission methods.
- **Distribution outside of ImageTrend internal mail.** Must be delivered direct; signature required; approved private carriers.
- **Electronic distribution.** No restriction to approved recipients within ImageTrend, but it is highly recommended that all information be strongly encrypted.
- **Storage.** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
- **Disposal/Destruction.** This is strongly encouraged: Should be in specially marked disposal bins on ImageTrend premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure.** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Terms

Appropriate measures

Definitions

To minimize risk to ImageTrend from an outside business connection, ImageTrend computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access ImageTrend corporate information, the amount of information at risk is minimized.

Configuration of ImageTrend-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot; instead, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within ImageTrend is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information

and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac, you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of ImageTrend.

Encryption

Secure ImageTrend Sensitive Information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a onetime password token to connect to ImageTrend's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that ImageTrend has control over for its entire distance. For example, all ImageTrend networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. ISDN lines to employees' homes are private links. ImageTrend also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies with which ImageTrend has established private links include all announced acquisitions and some short-term temporary links

PHYSICAL SECURITY OF OFFICE AND HOSTING SITE

Entrances

Facility and office entrances are kept to a minimum to control access. ImageTrend's main entrance is planned with access control systems and procedures in mind. Reception desk and other controls help to maintain security at ImageTrend's front entrance. The other entrances at the ImageTrend office are only accessible by employees with keys.

Access Controls

At every perimeter entrance, locking devices and controls are in place to ensure security is sustained. Key control is an essential part to ImageTrend's access control. Only ImageTrend employees are given a key that cannot be replicated. Before 8:00 am and after 5:00pm all ImageTrend entrances are locked. To get in or out before 8:00 am or after 5:00pm employees need to unlock the door to enter, and then relock the entrance behind them.

Exterior Security

ImageTrend equips the building with security cameras that run 24/7. These security cameras monitor activities outside the building to provide views of approaching pedestrian and vehicular traffic, building entrances, and departing pedestrian and vehicular traffic.

Physical Security of Hosting Site

All visitors of Implex.net are greeted and asked to sign in with photo ID. The visitors are escorted around the facility by an Implex.net employee. The Implex.net site has video surveillance and two controlled doors with key card access.

All visitor information, not just the sensitive information, is restricted to Implex.net developers, network operations personnel and other qualified employees (such as billing clerks or customer care representatives). Finally, the servers on which Implex.net stores personally identifiable information are kept in a secure location.

The DataSafe is Implex.net's main data center where they collocate servers and host client web sites on their shared servers. The entry to the Implex.net DataSafe was built inside a bank vault and is thoroughly encased by 21" reinforced concrete walls. The vault doors are fully functional.

REMOTE ACCESS POLICY

The purpose of this policy is to define standards for connecting to ImageTrend's network from any host. These standards are designed to minimize the potential exposure of ImageTrend to damages that may result from unauthorized use of ImageTrend resources. Damages include the loss of sensitive or company confidential data, loss of intellectual property, damage to public image, damage to critical ImageTrend internal systems, etc.

Scope

This policy applies to all ImageTrend employees, contractors, vendors and agents with an ImageTrend-owned or personally-owned computer or workstation used to connect to the ImageTrend network. This policy applies to remote access connections used to do work on behalf of ImageTrend, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH and cable modems, etc.

Policy

General

It is the responsibility of ImageTrend employees, contractors, vendors and agents with remote access privileges to ImageTrend's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ImageTrend.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods and of acceptable use of ImageTrend's network:

- Acceptable Encryption Policy
- Virtual Private Network (VPN) Policy
- Wireless Communications Policy
- Acceptable Use Policy

For additional information regarding ImageTrend's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases whenever possible. Use of a username/password combination is acceptable for access when DACL's are applied. For information on creating a strong passphrase see the Password Policy.

- At no time should any ImageTrend employee provide their login or email password to anyone, not even family members.
- ImageTrend employees and contractors with remote access privileges must ensure that their ImageTrend-owned or personal computer or workstation, which is remotely connected to ImageTrend's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- ImageTrend employees and contractors with remote access privileges to ImageTrend's corporate network must not use non-ImageTrend email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct ImageTrend business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the ImageTrend network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
- All hosts that are connected to ImageTrend internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
- Personal equipment that is used to connect to ImageTrend's networks must meet the requirements of ImageTrend-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the ImageTrend production network must obtain prior approval from Remote Access Services and InfoSec.

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol (CHAP) is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: being logged into the Corporate network via a local Ethernet connection and dialing into AOL or other Internet service provider (ISP); being on an ImageTrend-provided Remote Access home network and connecting to another network (such as a spouse's remote access); or configuring an ISDN router to dial into ImageTrend and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is another form of high-speed Internet access. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that can go incrementally from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network (ISDN): BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to ImageTrend's corporate network through a non-ImageTrend controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-ImageTrend network (such as the Internet or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into ImageTrend's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

ROLES AND RESPONSIBILITIES

Roles of system administrators in terms of their responsibility for defining and securing access for users are as follows:

Role	Responsibilities
Administrators (X-Team)	Full access to infrastructure, operating systems and supporting applications
Implementation	Full control of code, database tables and supporting applications
Level 1 Support	User level access to the ImageTrend application
Level 2 Support	Admin level access to the ImageTrend application and limited access to the supporting applications
Level 3 Support	SuperAdmin rights to the ImageTrend application read rights to the database and can change accounts and permissions

INCIDENT REPORT MECHANISM

Effective response and collective action are required to counteract security violations and activities that lead to security breaches. ImageTrend shall provide timely and appropriate notice to affected clients when there is reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information, typically maintained in an electronic format by ImageTrend.

Purpose

The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations. It is important to distinguish between problems that stem from mistakes or miscommunications and true security incidents that involve either malicious intent or intent to circumvent security measures

Scope

Attacks on ImageTrend resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on ImageTrend systems and/or on ImageTrend networks to appropriate authorities is a requirement of all persons affiliated with ImageTrend in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

General

Suspected or confirmed information security breaches must be reported to ImageTrend. ImageTrend will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform the IT Manager and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the IT Manager will consult with the appropriate ImageTrend employees to develop the response and make the final determination if a public notification of the event is warranted.

Procedures

The entity responsible for support of the system or network under attack is expected to:

- Report the attack to their management and to the IT Manager
- Block or prevent escalation of the attack, if possible
- Follow instructions communicated from the IT Manager in subsequent investigation of the incident and preservation of evidence
- Implement recommendations from the IT Manager
- Repair the resultant damage to the system

Internal Notifications

ImageTrend's employees will report serious computer security breaches to the IT Manager in a timely manner. The IT Manager will consult with one or more VP's as appropriate, and decides if the Management Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach.

External Notification

Determination of External Notification

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

- Physical possession (lost or stolen device?)
- Credible evidence the information was copied/removed
- Length of time between intrusion and detection

- Purpose of the intrusion was acquisition of information
- Credible evidence the information was in a useable format
- Ability to reach the affected individuals
- Applicable University policy, and/or local, state, or federal laws

External Notification

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

- Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists. The letter will be developed by the department responsible for the system experiencing the breach, and approved by the Management Team and others as appropriate. The excessiveness of cost consideration will be the decision of the IT Manager, Management Team, and President for.

If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

- Personal e-mail notices (provided addresses are available), developed by the department responsible for the system experiencing the breach, and approved by the IT Manager, Management Team, and other administrators as appropriate.
- A press release to media, to be written by Marketing and approved by the IT Manager, and other administrators as appropriate.
- An informational web site, developed and hosted by the department responsible for the system experiencing the breach, and approved by the IT Manager, Management Team, and others as appropriate, with a conspicuous link in the ImageTrend News area.
- All expenses associated with external notification will be the responsibility of the department responsible for the system that experienced the security breach.

SUPPORT SERVICES

ImageTrend provides both support for their applications and hosting as contracted. Support includes technical diagnosis and fixes of technology issues involving software and server hardware. ImageTrend has a broad range of technical support and proposes to provide service in the areas of:

- Website Hosting and Support
- Web Application Development/Enhancement
- Database Administration/Support
- Project Management
- Systems Engineering/Architecture

Product Support

ImageTrend will provide ongoing support as contracted after installation for the customer. This includes continued attention to product performance and general maintenance. ImageTrend offers multi-level technical support, based on level-two user support by accommodating both the general inquiries of the administrators and those of the system users. We will give the administrators the ability to field support for the system as the first level of contact while providing them the option to refer inquiries directly to ImageTrend.

ImageTrend's Support Team is available 24/7 at support@imagetrend.com and www.imagetrend.com/support as well as Monday through Friday from 7:00 am to 7:00 pm CST at:

Toll Free: 1-888-469-7789

Phone: 952-469-1589

Support Desk

ImageTrend offers an online support system, Support Desk, which incorporates around-the-clock incident

reporting of all submitted tickets to ImageTrend's support desk specialists. Once a client submits a support ticket, he or she can easily track its progress with a secure login, promoting a support log for the client and ImageTrend's support team. The system promotes speedy resolution by offering keyword-based self-help services and articles in the knowledgebase, should clients wish to bypass traditional support services. Ticket tracking further enhances the efforts of Support Desk personnel by allowing them to identify patterns which can then be utilized for improvements in production, documentation, education and frequently asked questions to populate the knowledgebase. The support ticket tracking system ensures efficient workflow for the support desk specialists while keeping users informed of their incident's status. Support patterns can be referenced to populate additional knowledgebase articles.

Upgrades and New Version Releases

ImageTrend offers updates and new version releases to customers subscribing to our support agreements. On average, these updates occur once a quarter. These updates offer new product enhancements and improvements. Customers are notified in advance of these potential changes in order for them to be aware of any impact this may have on them and to schedule the upgrade. The Fire Bridge, if hosted at our facilities, is upgraded by our personnel; however clients are notified prior to the upgrade for scheduling purposes. If the Fire Bridge is hosted at your facilities, then we assist in the upgrade either through remote login or an onsite visit if required (incurs travel costs).

The contents of the updates are determined by customer request levels and necessity. The EDS Users Group, comprised of field EMT's and Paramedics, has also been instrumental in providing insight for determining the necessity and value of requested product enhancements.

ImageTrend support agreements include software updates, so that applications continually offer the latest technology and provide new features. We encourage all clients to take advantage of these updates. Products will be maintained for the client as long as they have a valid support agreement.

X-Team Support

In addition to our standard services, ImageTrend's X-Team is available for after-hour's emergency support. Our X-Team will receive notifications of issues submitted to our Online Support Desk. If an issue is deemed non-critical by the X-team they may elect to respond during normal business hours or charge for after hour's resolution.

Problem Escalation and Resolution

ImageTrend has support available for clients via telephone, Support Desk and/or electronic mail during ImageTrend's normal business hours (7:00 a.m. to 7:00 p.m. Central Standard Time, Monday through Friday, excluding holidays). The Project Manager will address operational issues on an ongoing basis. Senior Management will handle issues requiring further discussion and resolution.

Incident Reporting

Malfunctions. ImageTrend makes all efforts to correct malfunctions that are documented and reported by the Client. ImageTrend acknowledges receipt of a malfunction report from a Client and acknowledges the disposition and possible resolution thereof according to the Service Level Agreement. If the Malfunction reported prevents all useful work from being done, or disables major functions from being performed, we undertake immediate corrective action to remedy the reported issue. If the malfunction reported represents a non-mission critical issue, reasonable corrective action to remedy the malfunction within three business days will be taken. If the malfunction reported disables only non-essential functions, resulting in degraded operations, we undertake reasonable corrective action to remedy the reported malfunction within a reasonable time period.

Submission. All support requests received by either direct phone contacts, Support Desk and support@imagetrend.com are recorded by client, incident description and disposition into our support log.

Support Log

Information regarding outstanding problems, fixes, modifications and improvements will be available to the Client electronically and published on a regular basis to a Project Support Log which will be available for Client's access.

ImageTrend University

ImageTrend provides online education materials for their products as self-guided tutorials to all clients with support agreements. These online support and educational materials can be found at ImageTrend University via your ImageTrend application. ImageTrend recently started implementing ImageTrend University throughout its solutions to promote ongoing education and training of our solutions. When accessing ImageTrend University through the application, users can view educational videos, manuals, quick guides and workbooks to assist them in better understanding our software and support train-the-trainer sessions. These have been very useful as both refresher and initial education materials. A sample demonstration of ImageTrend University can be found at www.imagetrend.com/university.

System Documentation

ImageTrend provides the most up-to-date documentation, including administrator and user manuals and release notes for any upgrades. With a support agreement, this documentation, along with educational videos, PowerPoint presentations and other documents will be found at ImageTrend University, which can be accessed from the State Bridge application. Any provided documentation becomes the property of the client. ImageTrend will provide a full set of documentation at each location upon request. Documentation updates are available online at no cost.

System Maintenance

Change Request. When a client makes a change request, we apply that to other users and their needs to determine if it would be beneficial to others in the EMS community – from the local volunteer organization to the regional users to mid and large size cities and state governments. If the requested change would be beneficial to the product as a whole, it may be included in a version release. For client-specific requests, we seek further mutual understanding. Sometimes product understanding meets the intended outcome of the change request or a work around is found. If neither of these meets the needs of the client, we can establish a Statement of Work to customize the application for the specific client for additional fees.

Support Staff. ImageTrend's support staff is made up of EMS and Fire professionals who are well versed in the technical aspects of our products. They are either well trained on the software, have used it in the field, or are the developers of the system.



Attachment 6 – Cost Tables

Table 1: Summary of the Project Costs

Project Cost(s)	Total Cost (\$)
MEMIS Software Maintenance and Support Table 2	\$472,120.00
Future Initiatives Table 3 and 4	\$249,000.00
Total Cost	\$721,120.00

Table 2: Annual Software Maintenance/Support and Hosting

	(4/1/14-9/30/14)	(10/1/14-9/30/15)	(10/1/15-9/30/16)	(10/1/16-9/30/17)	(10/1/17-9/30/18)	(10/1/18-9/30/19)	Total
MEMIS annual maintenance and support	\$29,120.00	\$58,240.00	\$58,240.00	\$58,240.00	\$58,240.00	\$58,240.00	\$320,320.00
MEMIS Annual Hosting	\$13,800.00	\$27,600.00	\$27,600.00	\$27,600.00	\$27,600.00	\$27,600.00	\$151,800.00
Grand Total maintenance/support, and hosting	\$42,920.00	\$85,840.00	\$85,840.00	\$85,840.00	\$85,840.00	\$85,840.00	\$472,120.00



Table 3: Future Initiatives – Rate Card

Resource Type	Not-to-Exceed Hourly Rate (\$)
Project management	\$125.00
Business analysts	\$125.00
System analysts	\$125.00
Programmer/developers	\$125.00
System administrators	\$125.00
Database administrators	\$125.00
Q/A Manager	\$125.00
Security specialist	\$125.00
Testers	\$125.00
Technical writers	\$125.00
CM specialists	\$125.00
System Architects	\$125.00
Network engineer/administrator	\$125.00
Software Architects	\$125.00
CM specialists	\$125.00
Project assistants	\$125.00
Web developers	\$125.00
Application trainers	\$125.00
Others: (List) below:	

Notes:

The State may request additional Position Types, other than the Position Types listed above during the contract term.



Table 4: Future Initiatives- Optional Software/Modules

Description	One-Time Cost	(4/1/14-9/30/14)	(10/1/14-9/30/15)	(10/1/15-9/30/16)	(10/1/16-9/30/17)	(10/1/17-9/30/18)	(10/1/18-9/30/19)	Total
Custom Development Allowance	\$125/hour	TBD	TBD	TBD	TBD	TBD	TBD	TBD
Upgrade to Rescue Bridge	\$130,000.00	\$14,100.00	\$28,200.00	\$28,200.00	\$28,200.00	\$28,200.00	\$28,200.00	\$275,100.00
Field Bridge Statewide Site License	\$120,000.00	\$9,600.00	\$19,200.00	\$19,200.00	\$19,200.00	\$19,200.00	\$19,200.00	\$225,600.00
MARS Setup	\$15,000.00	\$6,000.00	\$12,000.00	\$12,000.00	\$12,000.00	\$12,000.00	\$12,000.00	\$81,000.00
Hospital Dashboard/Hospital Hub Setup and Access	\$24,000.00	\$1,920.00	\$3,840.00	\$3,840.00	\$3,840.00	\$3,840.00	\$3,840.00	\$45,120.00
Visual Informatics (Data Mining) Additional Cubes – Each Cube	\$6,000.00	\$480.00	\$960.00	\$960.00	\$960.00	\$960.00	\$960.00	\$11,280.00
Patient Registry Categories (Forms) – Each Category	\$25,000.00	\$2,750.00	\$5,500.00	\$5,500.00	\$5,500.00	\$5,500.00	\$5,500.00	\$55,250.00
License Management License	\$90,000.00	\$15,300.00	\$30,600.00	\$30,600.00	\$30,600.00	\$30,600.00	\$30,600.00	\$258,300.00
Resource Bridge Base Platform	\$60,000.00	\$16,000.00	\$32,000.00	\$32,000.00	\$32,000.00	\$32,000.00	\$32,000.00	\$236,000.00
Resource Bridge Additional Modules	See Price Breakdown Below							
Grand Total	\$	\$						



ImageTrend Price Breakdown

Hosting and Maintenance	Description	Qty	Price	Extended Price
	EMS State Bridge Annual Support 4/01/2014-9/30/2014	1	\$14,720.00	\$14,720.00
	EMS State Bridge Annual Hosting 4/01/2014-9/30/2014	1	\$10,200.00	\$10,200.00
	Visual Informatics (Data Mining) Annual Support 4/01/2014-9/30/2014	1	\$4,800.00	\$4,800.00
	Patient Registry (Trauma Bridge) Annual Support 4/01/2014-9/30/2014	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Hosting 4/01/2014-9/30/2014	1	\$3,600.00	\$3,600.00
	Total for Year Ending September 30, 2014:			\$42,920.00
	EMS State Bridge Annual Support 10/01/2014-9/30/2015	1	\$29,440.00	\$29,440.00
	EMS State Bridge Annual Hosting 10/01/2014-9/30/2015	1	\$20,400.00	\$20,400.00
	Visual Informatics (Data Mining) Annual Support 10/01/2014-9/30/2015	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Support 10/01/2014-9/30/2015	1	\$19,200.00	\$19,200.00
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2014-9/30/2015	1	\$7,200.00	\$7,200.00
	Total for Year Ending September 30, 2015:			\$85,840.00
	EMS State Bridge Annual Support 10/01/2015-9/30/2016	1	\$29,440.00	\$29,440.00
	EMS State Bridge Annual Hosting 10/01/2015-9/30/2016	1	\$20,400.00	\$20,400.00
	Visual Informatics (Data Mining) Annual Support 10/01/2015-9/30/2016	1	\$9,600.00	\$9,600.00
	Patient Registry (Trauma Bridge) Annual Support 10/01/2015-9/30/2016	1	\$19,200.00	\$19,200.00
Patient Registry (Trauma Bridge) Annual Hosting 10/01/2015-9/30/2016	1	\$7,200.00	\$7,200.00	
Total for Year Ending September 30, 2016:			\$85,840.00	
EMS State Bridge Annual Support 10/01/2016-9/30/2017	1	\$29,440.00	\$29,440.00	
EMS State Bridge Annual Hosting 10/01/2016-9/30/2017	1	\$20,400.00	\$20,400.00	
Visual Informatics (Data Mining) Annual Support 10/01/2016-9/30/2017	1	\$9,600.00	\$9,600.00	



	Patient Registry (Trauma Bridge) Annual Support 10/01/2016-9/30/2017	1	\$19,200.00	\$19,200.00	
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2016-9/30/2017	1	\$7,200.00	\$7,200.00	
	Total for Year Ending September 30, 2017:			\$85,840.00	
	EMS State Bridge Annual Support 10/01/2017-9/30/2018	1	\$29,440.00	\$29,440.00	
	EMS State Bridge Annual Hosting 10/01/2017-9/30/2018	1	\$20,400.00	\$20,400.00	
	Visual Informatics (Data Mining) Annual Support 10/01/2017-9/30/2018	1	\$9,600.00	\$9,600.00	
	Patient Registry (Trauma Bridge) Annual Support 10/01/2017-9/30/2018	1	\$19,200.00	\$19,200.00	
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2017-9/30/2018	1	\$7,200.00	\$7,200.00	
	Total for Year Ending September 30, 2018:			\$85,840.00	
	EMS State Bridge Annual Support 10/01/2018-9/30/2019	1	\$29,440.00	\$29,440.00	
	EMS State Bridge Annual Hosting 10/01/2018-9/30/2019	1	\$20,400.00	\$20,400.00	
	Visual Informatics (Data Mining) Annual Support 10/01/2018-9/30/2019	1	\$9,600.00	\$9,600.00	
	Patient Registry (Trauma Bridge) Annual Support 10/01/2018-9/30/2019	1	\$19,200.00	\$19,200.00	
	Patient Registry (Trauma Bridge) Annual Hosting 10/01/2018-9/30/2019	1	\$7,200.00	\$7,200.00	
	Total for Year Ending September 30, 2019:			\$85,840.00	
	Ongoing Annual Fees for Optional Years*:			\$85,840.00	
	<i>*May be subject to Consumer Price Index increases as defined in the contract.</i>				
	OPTIONAL	Custom Development Allowance - Requires Statement of Work. May incur additional Hosting and/or Support Fees. Up to 1500 hours billed as used.	1	\$187,500.00	
Upgrade to State Rescue Bridge		1	\$120,000.00		
Upgrade to State Rescue Bridge Annual Support		1	\$19,200.00		
Upgrade to State Rescue Bridge Annual Hosting		1	\$9,000.00		
Upgrade to State Rescue Bridge Project Management and Setup		1	\$10,000.00		
Field Bridge Statewide Site License		1	\$120,000.00		
Field Bridge Statewide Site License Annual Support		1	\$19,200.00		
MARS (Mapping and Reporting System) Setup		1	\$15,000.00		



MARS Annual Transactional Fee	1	\$12,000.00	
Hospital Dashboard Setup	1	\$24,000.00	
Hospital Dashboard Annual Support	1	\$3,840.00	
Visual Informatics (Data Mining) Cubes:			
Fire Cube	1	\$6,000.00	
Fire Cube Annual Support	1	\$960.00	
Trauma (Incident) Cube	1	\$6,000.00	
Trauma Cube Annual Support	1	\$960.00	
Resource Bridge Cube	1	\$6,000.00	
Resource Bridge Annual Support	1	\$960.00	
Patient Registry Categories (Forms):			
Trauma Follow-up Category	1	\$18,000.00	
Trauma Follow-up Annual Support	1	\$2,880.00	
Trauma Follow-up Annual Hosting	1	\$1,200.00	
STEMI Category	1	\$25,000.00	
STEMI Category Annual Support	1	\$4,000.00	
STEMI Category Annual Hosting	1	\$1,500.00	
Stroke Category	1	\$25,000.00	
Stroke Category Annual Support	1	\$4,000.00	
Stroke Category Annual Hosting	1	\$1,500.00	
Burn Category	1	\$25,000.00	
Burn Category Annual Support	1	\$4,000.00	
Burn Category Annual Hosting	1	\$1,500.00	
Submersion Category	1	\$25,000.00	
Submersion Category Annual Support	1	\$4,000.00	
Submersion Category Annual Hosting	1	\$1,500.00	
Rehabilitation Category	1	\$25,000.00	
Rehabilitation Category Annual Support	1	\$4,000.00	
Rehabilitation Category Annual Hosting	1	\$1,500.00	
License Management License Fee	1	\$80,000.00	
License Management Annual Support	1	\$21,600.00	



License Management Annual Hosting	1	\$9,000.00	
License Management Project Management and Setup	1	\$10,000.00	
Personnel Licensure for First Responder, EMT-B, EMT-Advanced / Intermediate, EMT-P Types	1	\$20,000.00	
Vehicles Licensure for Ambulances	1	\$5,000.00	
Services/Agency Licensure for Ground, Air and Private	1	\$20,000.00	
Payment Gateway (TBD)	1	\$10,000.00	
Resource Bridge Base Platform	1	\$50,000.00	
Resource Bridge Base Platform Annual Support	1	\$8,000.00	
Resource Bridge Base Platform Annual Hosting (99.99%)	1	\$24,000.00	
Resource Bridge Base Platform Project Management & Setup	1	\$10,000.00	
Resource Bridge Additional Modules (requires purchase of Resource Bridge Base Platform):			
Alert Manager Setup	1	\$15,000.00	
Alert Manager Annual Support	1	\$2,400.00	
Alert Manager Annual Hosting	1	\$3,000.00	
Inventory Setup	1	\$25,000.00	
Inventory Annual Support	1	\$4,000.00	
Inventory Annual Hosting	1	\$3,600.00	
Procurement Setup	1	\$50,000.00	
Procurement Annual Support	1	\$8,000.00	
Procurement Annual Hosting	1	\$4,800.00	
Bed Tracking (includes HavBED export) with Specialties Setup	1	\$30,000.00	
Bed Tracking Annual Support	1	\$4,800.00	
Bed Tracking Annual Hosting	1	\$4,800.00	
Diversion Status (with Regional Status) Setup	1	\$15,000.00	
Diversion Status Annual Support	1	\$2,400.00	
Diversion Status Annual Hosting	1	\$3,000.00	
Fatality Tracking Web Module Setup	1	\$50,000.00	
Fatality Tracking Web Module Annual Support	1	\$8,000.00	
Fatality Tracking Web Module Annual Hosting	1	\$4,800.00	



Fatality Tracking Mobile Setup	1	\$25,000.00	
Fatality Tracking Mobile Annual Support	1	\$4,000.00	
Fatality Tracking Mobile Annual Hosting	1	\$3,600.00	
MAPS API Setup	1	\$10,000.00	
MAPS API Annual Support	1	\$1,600.00	
MAPS API Annual Hosting	1	\$2,400.00	
Resource Request Setup	1	\$15,000.00	
Resource Request Annual Support	1	\$2,400.00	
Resource Request Annual Hosting	1	\$3,000.00	
Command Center Setup	1	\$30,000.00	
Command Center Annual Support	1	\$4,800.00	
Command Center Annual Hosting	1	\$4,800.00	
Command Post Setup	1	\$15,000.00	
Command Post Annual Support	1	\$2,400.00	
Command Post Annual Hosting	1	\$3,000.00	
Patient Tracking Web Module Setup	1	\$30,000.00	
Patient Tracking Web Annual Support	1	\$4,800.00	
Patient Tracking Web Annual Hosting	1	\$4,800.00	
Patient Tracking Mobile Setup	1	\$25,000.00	
Patient Tracking Mobile Annual Support	1	\$4,000.00	
Patient Tracking Mobile Annual Hosting	1	\$3,600.00	
Document Hub Setup	1	\$10,000.00	
Document Hub Annual Support	1	\$1,600.00	
Hospital Hub Setup	1	\$30,000.00	
Hospital Hub Annual Support	1	\$4,800.00	
Hospital Hub Annual Hosting	1	\$4,800.00	
Onsite Training Sessions @ \$1,500 per day per trainer	1	\$1,500.00	
Custom Development - Out of Scope billed at \$125.00 per hour - requires separate Statement of Work	TBD	\$125.00	

Notes:



- a. ImageTrend agrees to offer a 10% discount on all one-time fees. This discount is valid for 90 days after contract signature. This would allow the State to select any optional items that they would like to move forward with in the near future at the discounted rate.
- b. ImageTrend agrees to lock-in the discounted rate on the one-time fees for the STEMI, Stroke and Burn Categories of the Patient Registry System provided they are included in the contract and will pro-rate any Annual Fees based on the implementation date of these items to align with the State's fiscal Year (10/1-9/30).

The initial value of spending authority for future initiatives to the Contract is \$249,000.00. Actual funding for future initiatives will occur on a yearly basis, and there is no guarantee as to the level of funding, if any, available to the project. The State makes no guarantee that any additional license(s), optional software/modules or technical services will be procured. The state reserves the right to purchase additional license(s), optional software/modules or technical services through other State contracts.

The State shall have the right to hold back an amount equal to percent 10% of all amounts invoiced by Contractor for specified deliverables for future enhancements. The amounts held back shall be released to Contractor after the State has granted Final Acceptance.

Future enhancements must be dependent upon mutually agreed upon statement(s) of work (SOW) between the Contractor and the State of Michigan. Once agreed to, the Contractor must not be obliged or authorized to commence any work to implement a statement of work until authorized via a purchase order issued against this contract.

Each SOW will include:

1. Background
2. Project Objective
3. Scope of Work
4. Deliverables
5. Acceptance Criteria
6. Project Control and Reports
7. Specific Department Standards
8. Cost/Rate
9. Payment Schedule
10. Project Contacts
11. Agency Responsibilities
12. Location of Where the Work is to be performed
13. Expected Contractor Work Hours and Conditions

The parties agree that the Services/Deliverables to be rendered by Contractor pursuant to this Contract (and any future amendments of it) will be defined and described in detail in a SOW.