



STATE OF MICHIGAN ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 1
to
Contract Number MA24000000832

CONTRACTOR	i3-ImageSoft, LLC
	40 Burton Hills Blvd., Ste. 414
	Nashville 42 37215
	Tim Zarzycki
	586-942-8423
	tzarzycki@i3verticals.com
	VS0228803

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Jarrod Barron	DTMB
		517-249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY				
MSHDA Electronic Document Management System				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
May 31, 2024	May 31, 2029	5 - 12 Months	May 31, 2029	
PAYMENT TERMS		DELIVERY TIMEFRAME		
Net 45				
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$2,659,158.11	\$200,000.00	\$2,859,158.11		

DESCRIPTION

Effective 2/25/2025, the parties add \$200,000.00 for the services detailed in the attached Content Portal and Integration statement of work. The parties add the following language to the Contract:

"Accessibility Requirements.

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites, applications, content, and electronic documents. Due to a change in the law, the State is required to comply with specific accessibility standards for websites, applications, content and documents.

Starting 4/24/2026, throughout the Term, all websites, applications, software, content, and electronic documents, including but not limited to mobile applications, text, images, sounds, videos, controls, animations, links, and documents (including files in the following formats: PDF, word processing, presentation, and spreadsheet), created, provided, or made available by the Contractor under this Contract, must comply with WCAG 2.1 Level AA."

All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, and DTMB Central Procurement approval. Per Contractor, Agency, and DTMB Procurement approval.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
MSHDA	Mark Whitaker	517-335-9812	WhitakerM@michigan.gov
DTMB	Michael Weiszbrod	517-242-1272	WeiszbrodM@michigan.gov

STATEMENT OF WORK - IT CHANGE NOTICE

Project Title: MSHDA – i3 – Content Portal and Integration	Period of Coverage: 5/31/2024 - 5/21/2029
Requesting Department: MSHDA	Date: 2/24/2025
Agency Project Manager: Mark Whitaker	Phone: 517-335-9812
DTMB Project Manager: Michael Weiszbrod	Phone: 517-242-1272

BACKGROUND:

MSHDA and i3 have been engaged in a project to stand up a Hyland implementation for the Rental Development division per MA 24000000832. During this initiative, the need for a Portal was identified.

PROJECT OBJECTIVE:

In consultation with representatives from i3-ImageSoft, LLC. (“i3-ImageSoft” or “Contractor”) Professional Services, MSHDA has stated the following business needs:

- 1) MSDHA has requested “save as you go” functionality for external users. To meet these requirements, Jadu & i3-ImageSoft will install and configure the Hyland Content Portal hosted in the i3-ImageSoft Azure Cloud environment. The Portal will utilize the Jadu platform and will be integrated with MILogin and the existing OnBase solution to enable Customer’s external users to securely view relevant documents, submit documents, and complete forms as well as track missing documents related to an application by logging into a Jadu account. One (1) Eligibility Form will be configured with “save as you go” functionality to allow users to complete and submit at a later time.

SCOPE OF WORK:

Configure process to indicate required documentation to the submitting users.
Configure OnBase to receive incoming data from the form submission.

To implement the proposed Services, Jadu & i3-ImageSoft will undertake the following tasks:

- 1) Install OnBase and Jadu software and configure the Portal for document and form submission.
- 2) Configure Portal integration with MILogin.
- 3) Configure one (1) Eligibility Form with submissions into OnBase and one (1) Portal page for document/workflow viewing.
- 4) Configure connections between Jadu and Hyland OnBase/Workflow.
- 5) Update OnBase design to account for the Jadu integration.
 - a. Configure status updates from OnBase to the Portal to allow users the ability to see submission status
 - b. Configure process to indicate required documentation to the submitting users.
 - c. Configure OnBase to receive incoming data from the form submission.

- 6) Conduct system testing.
- 7) Provide two (2) training courses: Foundation (self-paced) and Practitioner (instructor led), maximum ten (10) delegates.
- 8) Conduct knowledge transfer session with System Administrator.
- 9) Assist with up to one (1) week additional User Acceptance Testing (“UAT”).

ASSUMPTIONS:

The following assumptions were made when estimating pricing for this Project Change Request (“PCR”):

- 1) Customer will provide resources for end user training.
- 2) The solution will be implemented in the i3-ImageSoft Cloud environment.
- 3) Customer acknowledges and agrees that i3-ImageSoft will engage Jadu., Inc. to provide certain software and support services to you in connection with this PCR.
- 4) Any development activities of solution automations (iScripts, eForms, etc.) are out of scope with this engagement. Any Solution automations are to be scoped and quoted separately.
- 5) A comprehensive requirements analysis or creation of a roadmap is not included.
- 6) Software and services not outlined above which are necessary to satisfy business requirements not yet discovered are excluded from scope.

DELIVERABLES:

Deliverables will not be considered complete until the Agency Project Manager has formally accepted them. Deliverables for this project include:

Hosted Portal utilizing the Jadu Platform integrated with the existing OnBase solution allowing external users to enter key data, upload/submit, and view documents/forms.

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. **Funds:** Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

PAYMENT SCHEDULE:

Payment will be made on a Satisfactory acceptance of each deliverable basis. DTMB will pay CONTRACTOR upon receipt of properly completed invoice(s) which shall be submitted to the billing address on the State issued purchase order not more often than monthly. DTMB Accounts Payable area will coordinate obtaining Agency and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date and must be approved by the Agency 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 DTMB within forty-five (45) days after receipt of properly completed invoices.

Contract Change Notice Cost Summary:

Contract Year	Annual Software Subscriptions	Implementation Service Fees	Total
Year 1 (5/30/2024 - 5/29/2025)	N/A	N/A	N/A
Year 2 (5/30/2025 - 5/29/2026)	\$45,000.00	\$20,000.00	\$45,000.00
Year 3 (5/30/2026 - 5/29/2027)	\$45,000.00	\$-	\$45,000.00
Year 4 (5/30/2027 - 5/29/2028)	\$45,000.00	\$-	\$45,000.00
Year 5 (5/30/2028 - 5/29/2029)	\$45,000.00	\$-	\$45,000.00
Change Notice Total	\$180,000.00	\$20,000.00	\$200,000.00

Product/Service Detail:

*Annual Software Subscriptions	
	Product
Jadu Portal (Annual Subscription)	
Jadu Portal for State Government – Small Agency (Up to 500 employees) – Single Department <ul style="list-style-type: none"> OnBase Connector Software WorkView Connector Software 	JADU-SGS_SUBS JADU-OBINT_SUBS JADU-WVINT_SUBS
OnBase (Annual Subscription)	
OnBase Integration for Hyland Content Portal OnBase WorkView Integration for Hyland Content Portal – OnBase API Only	HCPSGI1-SMS_SUBS HCPWVI-API_SUBS
Software and Support Subtotal	
Implementation Service Fees	
Professional Services	
Jadu Base 3 – On-premise Windows install, user training, auth adapter, integration setup, and one (1) form	JADU-BASE3-OPW

EXPENSES:

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

PROJECT CONTACTS:

The designated Agency Project Manager is:

Mark Whitaker
MSHDA
735 E. Michigan Avenue
Lansing Michigan 48912
517-335-9812
whitakerm@michigan.gov

The designated DTMB Project Manager is:

Michael Weiszbrod
DTMB
Agency Services
4125 W St Joe Hwy
Lansing Michigan 48917
517-242-1272
weiszbrodm@michigan.gov

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

Consultants will work at:

Contractor location

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.

PROJECT PLAN:

Project plan as outlined in MA 240000000832



STATE OF MICHIGAN PROCUREMENT
 Department of Technology, Management & Budget
 525 W. Allegan Street, Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **171-240000000832**
 between
 THE STATE OF MICHIGAN
 and

CONTRACTOR	i3-ImageSoft, LLC
	40 Burton Hills Blvd., Ste. 414
	Nashville, TN 37215
	Tim Zarzycki
	586-942-8423
	tzarzycki@i3verticals.com
	VS0228803

STATE	Program Manager	Various	MSHDA
	Contract Administrator	Jarrod Barron	DTMB
		517-249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: MSHDA Electronic Document Management System			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
5/31/2024	5/31/2029	Five 1-Year, Through 5/31/2034	N/A
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45			
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
New contract established via ITN 171-240000000017. Program Managers: 1. MSHDA: Mark Whitaker, whitakerm@michigan.gov, 517-335-9812 2. DTMB: Michael Weiszbrod, weiszbrodm@michigan.gov, 517-242-1272			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			\$2,659,158.11

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Jarrod Barron – IT Category Specialist
Name & Title

DTMB – Central Procurement Services
Agency

Date

SOFTWARE CONTRACT TERMS AND CONDITIONS

These Software Contract Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this “Contract”) are agreed to between the State of Michigan (the “State”) and i3-ImageSoft, LLC (“Contractor”), a Delaware limited liability company. This Contract is effective on May 31, 2024 (“Effective Date”), and unless terminated, will expire on May 31, 2029 (the “Term”).

This Contract may be renewed for up to five additional 1-year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via a Change Notice.

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

“**Acceptance**” has the meaning set forth in **Section 9**.

“**Acceptance Tests**” means such tests as may be conducted in as described in **Section 9** and any applicable Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

“**Access**” means (1) the ability and means to enter a restricted or locked area, room, or physical container containing State Data; or (2) the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain the information or knowledge of the information the system contains, or to control system components and functions (including physical or technical controls, or having the ability to modify or bypass any or all security controls).

“**Affiliate**” of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term “control” (including the terms “controlled by” and “under common control with”) means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

“**Allegedly Infringing Materials**” has the meaning set forth in **Section 18**.

“**Authorized Users**” means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

“**Business Day**” means a day other than a Saturday, Sunday, or other day on which the State is authorized or required by law to be closed for business.

“**Business Requirements Specification**” means the initial specification setting forth the State’s business requirements regarding the features and functionality of the Software, as set forth in a Statement of Work.

“**Contract Change**” has the meaning set forth in **Subsection 2.2**.

“**Change Notice**” means a writing executed by the parties to the Contract memorializing a change to the Contract.

“**Change Proposal**” has the meaning set forth in **Subsection 2.2**.

“**Change Request**” has the meaning set forth in **Subsection 2.2**.

“**Confidential Information**” has the meaning set forth in **Subsection 22.1**.

“**Configuration**” means State-specific changes made to the Software without Source Code or structural data model changes occurring.

“**Contract**” has the meaning set forth in the preamble.

“**Contract Administrator**” is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party’s Contract Administrator will be identified in Schedule A or subsequent Change Notices.

“**Contractor**” has the meaning set forth in the preamble.

“**Contractor’s Bid Response**” means the Contractor’s proposal submitted in response to the Solicitation.

“**Contractor Hosted**” means the Hosted Services and the Operating Environment are provided by Contractor or one or more of its Permitted Subcontractors.

“**Contractor Personnel**” means all employees of Contractor, or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

“**Contractor Project Manager**” means the individual appointed by Contractor and identified in Schedule A or subsequent Change Notices to serve as the primary contact, to monitor and coordinate the day-to-day activities of this Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

“**Customization**” means State-specific changes to the Software’s underlying Source Code or structural data model changes.

“**Deliverables**” means the Software, Documentation, any hardware, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in a Statement of Work and all Work Product.

“**Deposit Material**” refers to material required to be deposited pursuant to **Section 28**.

“**Digital Accessibility Standards**” means the accessibility standards provided in the SOM Digital Standards, located at <https://www.michigan.gov/standards>.

“**Disaster Recovery Plan**” refers to the set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations and to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives.

“**Documentation**” means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Deliverable.

“**DTMB**” means the Michigan Department of Technology, Management and Budget.

“**Effective Date**” has the meaning set forth in the preamble.

“**Fees**” means the fees set forth in the Pricing Schedule attached as **Schedule B**.

“**Financial Audit Period**” has the meaning set forth in **Subsection 23.1**.

“**Harmful Code**” means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

“Hosted Services” means the hosting, management and operation of the: Operating Environment, Software, other services (including support and subcontracted services), and related resources for access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“Implementation Plan” means the schedule included in a Statement of Work setting forth the sequence of events for the performance of Services under a Statement of Work, including the Milestones and Milestone Dates.

“Integration Testing” has the meaning set forth in **Section 9**.

“Intellectual Property Rights” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable law in any jurisdiction throughout the world.

“Key Personnel” means any Contractor Personnel identified as key personnel in the Contract.

“Loss or Losses” means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“Maintenance Release” means any update, upgrade, release, or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, general enhancements, improvements, or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“Milestone” means an event or task described in the Implementation Plan under a Statement of Work that must be completed by the corresponding Milestone Date.

“Milestone Date” means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under a Statement of Work.

“New Version” means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“Nonconformity” or **“Nonconformities”** means any failure or failures of a Deliverable, to conform to the requirements of this Contract.

“Open Source Components” means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

“Operating Environment” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

“PAT” means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software

products, such as websites, applications, software and associated content, conform to the Digital Accessibility Standards.

“**Permitted Subcontractor**” means any third party hired by Contractor to perform Services for the State under this Contract or that will have Access to or have the ability to control access to State Data or both.

“**Person**” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association, or other entity.

“**Pricing Schedule**” means the schedule attached as **Schedule B**.

“**Process**” means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. “**Processing**” and “**Processed**” have correlative meanings.

“**Representatives**” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“**Services**” means any of the services, including but not limited to, Hosted Services, installation, configuration, implementation, and/or Support Services, that the Contractor is required to or otherwise does provide under this Contract.

“**Service Level Agreement**” means the schedule attached as **Schedule D**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

“**Site**” means any physical location(s) designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Deliverable, if applicable.

“**Software**” means Contractor's software as set forth in a Statement of Work, and any Third-Party Components, Maintenance Releases or New Versions provided to the State and any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract. If Contractor Hosted, Software includes Contractor's Operating Environment.

“**Solicitation**” means the State's request to solicit responses for a Solution under this Contract.

“**Solution**” means Deliverables and Services singularly or in any combination thereof, as applicable, set forth in a Statement of Work.

“**Source Code**” means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

“**Specifications**” means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, Solicitation or Contractor's Bid Response, if any, for such Software, or elsewhere in a Statement of Work.

“**State**” means the State of Michigan.

“**State Data**” has the meaning set forth in **Section 21**.

“**State Hosted**” means the Operating Environment is not provided by Contractor or one or more of its Permitted Subcontractors.

“State Materials” means all materials and information, including but not limited to documents, data, know-how, ideas, methodologies, specifications, software, hardware, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“State Program Managers” are the individuals appointed by the State, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Deliverables; and (c) perform other duties as may be specified in a Statement of Work. Program Managers will be identified in Schedule A or subsequent Change Notices.

“State Systems” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

“Statement of Work” means any statement of work entered into by the parties and incorporated into this Contract. The initial Statement of Work is attached as **Schedule A**.

“Stop Work Order” has the meaning set forth in **Section 15**.

“Support Services” means the maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

“Technical Specification” means, with respect to any Software, the document setting forth the technical specifications for such Software and included in a Statement of Work.

“Term” has the meaning set forth in the preamble.

“Testing Period” has the meaning set forth in **Section 9**.

“Third-Party Components” means all components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Contractor’s Software Bill of Materials, in an applicable Statement of Work or elsewhere in this Contract, or as otherwise required by this Contract, including without limitation as part of the State’s Security Accreditation Process defined in Schedule E – Data Security Requirements.

“Transition Period” has the meaning set forth in **Section 16**.

“Transition Responsibilities” has the meaning set forth in **Section 16**.

“Unauthorized Removal” has the meaning set forth in **Subsection 2.5**.

“Unauthorized Removal Credit” has the meaning set forth in **Subsection 2.5**.

“User Data” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, including information that identifies the State devices or equipment and any location information even if not input by a user except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input without the inclusion of user derived information or additional user input, with the exception of any identifying information.

“Warranty Period” means the 90 calendar-day period commencing on the date of the State's Acceptance of the Software for which Support Services are provided free of charge.

“Work Product” means everything made or created by Contractor specifically and solely for the State and which is not generally available to Contractor’s other customers that Contractor is required to, or otherwise does,

provide to the State under this Contract including but not limited to Customizations, application programming interfaces, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Duties of Contractor. Contractor will provide the Solution pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide the Solution in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement(s) of Work.

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each party's Contract Administrator. The term of each Statement of Work will commence on the parties' full execution of a Statement of Work and terminate when the parties have fully performed their obligations, unless earlier terminated in accordance with the terms of this Contract. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 16**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Contract, including without limitation changes to the Solution or adding a new Statement of Work (each, a "**Contract Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this Section.

(a) As soon as reasonably practicable, and in any case within 20 Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

- (i) a written description of the proposed Changes to any part of the Solution;
- (ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any addition or modification to the Solution; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;
- (iii) any additional State Resources Contractor deems necessary to carry out such Changes; and
- (iv) any increase or decrease in Fees resulting from the proposed Changes, which increase, or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within 30 Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications each parties' Contractor Administrator will sign a Change Notice.,

(c) However, if the parties fail to enter into a Change Notice within 15 Business Days following the State's response to a Change Proposal, the State may, in its discretion:

- (i) require Contractor to perform or provide the Solution under the existing Statement of Work without the Change;
- (ii) require Contractor to continue to negotiate a Change Notice;
- (iii) initiate a Dispute Resolution Procedure; or
- (iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Subsection 16.1**.

(d) No Change will be effective until the parties have executed a Change Notice. Notwithstanding the foregoing, no Change Notice executed after the Effective Date will be construed to amend or modify this Contract in any way, unless it specifically states its intent to do so and cites the section or sections amended. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Solution as described in this Contract are considered part of the Solution and, thus, will not be

considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Nonconformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

2.3 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) ensure that such Contractor Personnel have the legal right to work in the United States;

(ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and

(iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have Access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any 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. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor.

(a) Contractor Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.

(c) Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor Project Manager; or

(ii) the State consents in writing to any removal requested by Contractor in writing; or

- (iii) the Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.
- (d) Upon the occurrence of any event set forth in **Subsections 2.4(c)(i-iii)** above, Contractor will promptly replace its Contractor Project Manager. Such replacement will be subject to the State's prior written approval.

2.5 Contractor's Key Personnel.

- (a) The State has 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 will notify the State of the proposed assignment, introduce the individual to the State Program Managers or their designees, and 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 will provide a written explanation including reasonable detail outlining the reasons for the rejection.
- (b) Contractor will not remove any Key Personnel from their assigned roles on this 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**"). An Unauthorized Removal 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. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract.
- (c) It is further acknowledged that an Unauthorized Removal may interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to determine and remedy 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 (i.e., something outside of Contractor's control) in respect of which the State does not elect to exercise its rights under **Section 16**, Contractor will issue to the State an amount equal to \$25,000 per individual (each, an "**Unauthorized Removal Credit**").
- (d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection 2.5(c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to provide Services to the State under this Contract. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

- (a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing the Solution, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;
- (b) be responsible for all fees and expenses payable to, by or on behalf of each subcontractor and Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and
- (c) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the United States.

3. Notices. All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received or as follows: (a) when verified by written receipt if sent by personal delivery or overnight courier (delivery for overnight courier being one (1) Business Day with tracking); (b) the lesser of when received or ten (10) Business Days if sent by mail without verification of receipt; or (c) when verified by automated receipt, confirmation, or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
--------------	-------------------

Jarrod Barron 320 S. Walnut Lansing, MI 48909 BarronJ1@michigan.gov 517-249-0406	Tim Zarzycki i3-ImageSoft, LLC 40 Burton Hills Blvd., Ste. 414 Nashville, TN 37215 tzarzycki@i3verticals.com 586-942-8423
--	--

4. Insurance. Contractor must maintain the minimum insurances and in the amounts identified in the Insurance Schedule attached as **Schedule C**.

5. Terms of Use of the Software.

5.1 Subscription.

(a) During the Term and such additional periods, if any, the State may:

(i) access and use the Software, including in operation with other software, hardware, systems, networks and services, for the State's governmental purposes, including for Processing State Data;

(ii) generate, print, copy, upload, download, store and otherwise Process all GUI, audio, visual, digital and other output, displays and other content as may result from any access to or use of the Software;

(iii) prepare, reproduce, print, download and use a reasonable number of copies of the Specifications and Documentation for any use of the Software under this Contract; and

(iv) access and use the Software for all such non-production uses and applications as may be necessary or useful for the effective use of the Software hereunder, including for purposes of analysis, development, configuration, integration, testing, training, maintenance, support and repair, which access and use will be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Subsection 5.4** below.

5.2 Restrictions. The State will not: (a) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make the Software available to any third party, except as expressly permitted by this Contract or in any Statement of Work; or (b) use or authorize the use of the Software or Documentation in any manner or for any purpose that is unlawful under applicable Law.

5.3 Fees. The State will pay Contractor the corresponding Fees set forth in a Statement of Work or Pricing Schedule for all Authorized Users access and use of the Software. Such Fees will be Contractor's sole and exclusive remedy for use of the Software, including any excess use.

5.4 Certification. To the extent that a License granted to the State is not unlimited, Contractor may request written certification from the State regarding use of the Software for the sole purpose of verifying compliance with this **Section**. Such written certification may occur no more than once in any 24 month period during the Term of the Contract. The State will respond to any such request within 45 calendar days of receipt. If the State's use is greater than contracted, Contractor may invoice the State for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in **Schedule B**, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

5.5 State License Grant to Contractor. The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or

division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work. Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

6. Third-Party Components. At least 30 days prior to adding new third-party components, (or less if required by law or regulatory reasons), Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any third-party components included in the Software. Contractor is responsible for ensuring that all Third-Party Components are properly licensed for the State's use during the Term of the Contract.

7. Intellectual Property Rights

7.1 Ownership Rights in Software

(a) For purposes of this **Section 7** only, the term "Software" does not include Customizations.

(b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Subsection 7.1(c)**:

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and

(ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(c) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to State Materials, User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

7.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including any Intellectual Property Rights incorporated and developed solely for State which constitutes Work Product. Except for the licenses granted herein, no Intellectual Property Rights that are part of any Deliverable, as a whole or in part, that are used or integrated with any other Contractor developments, creations, works, or products of Contractor as generally provided to other customers or clients of Contractor will transfer to State and State will take no ownership in such Intellectual Property Rights. In furtherance of the foregoing and as applicable:

(a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any Work Product, do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including any Intellectual Property Rights; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the Work Product.

8. Software Implementation.

8.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise make available, and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan.

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to provide the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in a Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery of the Software. If the State is responsible for Site preparation, and having all devices, computers, and systems with relevant connectively available for purposes of the Software. Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

9. Software Acceptance Testing.

9.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, or in the case of Contractor Hosted Software, when Contractor notifies the State in writing that the Solution is ready for use, Acceptance Tests will be conducted as set forth in this **Section 9** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following installation of the Software, or the receipt by the State of the notification referenced in **Subsection 9.1(a)**, and be conducted diligently for up to 30 Business Days, or such other period as may be set forth in a Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in a Statement of Work or, if a Statement of Work does not specify, the State, provided that:

- (i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and
- (ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

9.2 Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing, unless otherwise provided in a Statement of Work.

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in this **Section**.

(b) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Nonconformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within 10 Business Days, correct such Nonconformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within 15 Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Nonconformity in the tested Software.

(a) If such notice is provided by either party and identifies any Nonconformities, the parties' rights, remedies, and obligations will be as set forth in **Subsection 9.4** and **Subsection 9.5**.

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Nonconformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have 30 Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Nonconformities, on the completion of which the State will, as appropriate:

- (i) notify Contractor in writing of Nonconformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Subsection 9.4** and **Subsection 9.5**; or
- (ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State Program Managers or their designees.

9.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Nonconformities and re-deliver the Software, in accordance with the requirements set forth in the Contract. Redelivery will occur as promptly as commercially possible and, in any case, within 30 Business Days following, as applicable, Contractor's:

- (a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or
- (b) receipt of the State's notice under **Subsection 9. (a)** or **(c)(i)**, identifying any Nonconformities.

9.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Nonconformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

- (a) continue the process set forth in this **Section 9**;
- (b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or
- (c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract in accordance with **Section 16**.

9.6 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the Software under **Subsection 9.3(b)**, or **(c)(ii)**.

10. Non-Software Acceptance.

10.1 All other non-Software Deliverables are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("State Review Period"), unless otherwise provided in the Statement of Work. If the non-Software Deliverables are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the non-Software Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the non-Software Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16**.

10.2 Within 10 Business Days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any non-Software Deliverables, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable non-Software Deliverables to the State. If acceptance with deficiencies or rejection of the non-Software Deliverables impacts the content or delivery of other non-completed non-Software Deliverables, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

10.3 If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may provide the non-Software Deliverables and recover the difference between the cost to cure and the Contract price.

11. Assignment. Contractor may not assign this Contract or any of its rights or delegate any of its duties or obligations hereunder, voluntarily, or involuntarily, whether by merger (regardless of whether it is the surviving or disappearing entity), conversion, consolidation, dissolution, or operation of law to any other party without the prior written approval of the State. Upon notice to Contractor and Contractor confirmation that the Services are transferable and Contractor can continue to meet the obligations of this Contract without undue interruption, modification, or change, the State may assign in whole or in part, its rights or responsibilities under this Contract to another Michigan State governmental entity, if such assignment is made reasonably necessary by operation of controlling law or regulation. If it is reasonably determined that a novation of the Contract to a third party is necessary, practicable, and Contractor confirms performance of its obligations hereunder can reasonably be continued without interruption, then Contractor will agree to the novation in writing.

12. Change of Control. Contractor will notify the State, within 60 calendar days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

- (a) a sale of more than 50% of Contractor's stock;
- (b) a sale of substantially all of Contractor's assets;
- (c) a change in a majority of Contractor's board members;
- (d) consummation of a merger or consolidation of Contractor with any other entity;
- (e) a change in ownership through a transaction or series of transactions;
- (f) or the board (or the stockholders) approves a plan of complete liquidation.

A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

13. Ordering, Invoices and Payment.

13.1 Authorizing Document. The document for the Contract will be a delivery order. No work should start until the delivery order is received by the Contractor.

13.2 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for the Solution provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.3 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount, which the parties will attempt to resolve within 60 days of notice of disputed amount. The State will notify Contractor of any dispute within 45 days of receipt of invoice. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Deliverables. Contractor's acceptance of final payment by the State constitutes 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 disputed.

13.4 The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment.

13.5 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off or withhold any amount, disputed in good faith, then due and owing which is payable by the State to Contractor under this Contract.

13.6 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if the Solution purchased under this Contract is for the State's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

13.7 Pricing/Fee Changes. Throughout the Term, all Pricing set forth in this Contract will be as set forth in **Schedule B – Pricing Schedule** and will not be increased, unless the State requires additional licenses, in which case the amount of fee per license the additional licenses will also remain fixed at the rates set forth in **Schedule B – Pricing Schedule**.

14. Liquidated Damages.

14.1 The parties understand and agree that any liquidated damages (which includes but is not limited to applicable credits) set forth in this Contract are reasonable estimates of the State's damages in accordance with applicable law.

14.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event.

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause and the State will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

14.4 For amounts due the State as liquidated damages, may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

15. Stop Work Order. The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 60 calendar days, or any longer period as agreed to by Contractor in writing, the State will either:

- (a) issue a notice authorizing Contractor to resume work, or
- (b) terminate the Contract or delivery order. The State will not pay for activities that have been suspended, Contractor's lost profits, or any additional compensation during a stop work period.

The State will be responsible to pay all costs and Fees incurred for Services rendered to the State by Contractor up and until the notice of suspension or termination.

16. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

16.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

- (a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:

- i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;
 - (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or
 - (iii) breaches any of its material duties or obligations under this Contract and fails to cure such default within 15 calendar days following written notice from the State. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.
- (b) If the State terminates this Contract under this **Subsection 16.1**, the State will issue a termination notice specifying whether Contractor must:
- (i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 60 calendar days of the actual date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or
 - (ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Subsection 16.2**.
- (c) The State will only pay for amounts due to Contractor for Services actually rendered and delivered or accepted by the State on or before the date of termination, subject to the State's right to set off any good faith disputed amounts owed. If the State terminates this Contract for an actual default by Contractor, then Contractor will promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause due to Contractor's uncured default up to and limited to two times the total annual cost of the Fees, including administrative costs, attorneys' fees, court costs, and transition costs.

16.2 Termination for Convenience. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason or no reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must:

- (a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 60 calendar days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or
- (b) continue to perform in accordance with **Subsection 16.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

16.3 Transition Responsibilities.

- (a) Upon termination or expiration of this Contract for any reason, Contractor agrees, for a period of time, not to exceed 90 calendar days, (the "**Transition Period**"), provide reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees on the same terms and conditions herein. Such transition assistance may include but is not limited to:
 - (i) continuing to perform the Services at the established Contract rates and Fees;
 - (ii) taking reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee;
 - (iii) taking necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22**, including without limitation, the return or destruction of State Data at the conclusion of the Transition Period; and
 - (iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.
- (b) The parties will follow the transition plan attached as **Schedule G** as it pertains to both transition in and transition out activities.

17. Indemnification

17.1 General Indemnification. Contractor agrees to defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and

against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to:

- (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;
- (b) any infringement, misappropriation, or other violation of any Intellectual Property Right held and offered as part of the Services, or other alleged intellectual infringement right of any third party made against the State for a Deliverable from Contractor;
- (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) in performing the Services, which gives rise to a claim against the State by a third party; and
- (d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable), which gives rise to a claim against the State due to Contractor's act or omission.

17.2 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor of its obligation, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to:

- (a) regular updates on proceeding status from Contractor or Contractor's legal counsel;
- (b) participate in the defense of the proceeding, at State's sole cost, provided Contractor remains in control over any defense or settlement;
- (c) employ its own counsel at State's sole cost; and to
- (d) retain control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

17.3 The State is constitutionally prohibited from indemnifying Contractor or any third parties.

18. Infringement Remedies.

18.1 The remedies set forth in this Section are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

18.2 If any Deliverable, or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

- (a) procure for the State the right to continue to use such Deliverable, or component thereof to the full extent contemplated by this Contract; or
- (b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Deliverable and all of its components non-infringing while providing fully equivalent features and functionality.

18.3 If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

- (a) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Deliverable provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and
- (b) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to 6 months, if practicable and procurable, to allow the State to replace the affected features of the Deliverable without disruption.

18.4 If Contractor directs the State to cease using any Deliverable under **Subsection 18.3**, (without a reasonable replacement option, the State, at its sole discretion, will be entitled to declare such a direction from the Contractor to cease use a material breach of the Contract and may terminate this Contract under **Section 16**. Unless the claim arose against the Deliverable independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

- (a) Contractor's compliance with any Customizations, designs, specifications, or instructions of the State; or

(b) modification of the Deliverables by the State without the prior knowledge and approval of Contractor.

19. Disclaimer of Damages and Limitation of Liability.

19.1 The State's Disclaimer of Damages. THE STATE WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

19.2 The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

19.3 Contractor's Limitation of Liability and Disclaimer of Damages. IN NO EVENT WILL CONTRACTOR BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR BY STATUTE OR OTHERWISE, FOR ANY DAMAGES, CLAIMS, PROCEEDINGS, OR ALLEGATIONS RELATED TO OR ARISING UNDER THIS CONTRACT FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, PUNITIVE, EXEMPLARY, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

20. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 30 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

- (a) a criminal Proceeding;
- (b) a parole or probation Proceeding;
- (c) a Proceeding under the Sarbanes-Oxley Act;
- (d) a civil Proceeding involving:
 - (i) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or
 - (ii) a governmental or public entity's claim or written allegation of fraud; or
- (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

21. State Data.

21.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes:

- (a) User Data;
- (b) all data made available to Contractor for or during the provision of the Solution, including but not limited to all text, sound, video, image files, or software; and
- (c) any other data collected, used, Processed, stored, or generated in connection with the Solution, including but not limited to:
 - (i) personally identifiable information ("**PII**"), if any, collected, used, Processed, stored, or generated as the result of the Solution, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and
 - (ii) protected health information ("**PHI**"), if any, collected, used, Processed, stored, or generated as the result of the Solution, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations.

21.2 State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State.

21.3 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Solution, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Solution. Contractor must:

- (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss;
- (b) use and disclose State Data solely and exclusively for the purpose of providing the Solution, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law;
- (c) keep and maintain State Data in the United States and
- (d) not use, sell, rent, transfer, mine, distribute, commercially exploit, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. Contractor's misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795.

21.4 Third-Party Requests. Contractor will immediately notify the State upon receipt of any third-party requests which in any way might reasonably require Access to State Data. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. Contractor must provide such notification within twenty-four (24) hours from Contractor's receipt of the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State. Upon request by the State, Contractor must provide to the State, its proposed response to the third-party request with adequate time for the State to review, and, as it deems necessary, to revise the response, object, or take other action.

21.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable:

- (a) notify the State as soon as practicable but no later than 24 hours of becoming aware of such occurrence;
- (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;
- (c) in the case of PII or PHI, at the State's sole election:
 - (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or
 - (ii) reimburse the State for any costs in notifying the affected individuals;
- (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;
- (e) perform or take any other actions required to comply with applicable law as a result of the occurrence;
- (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;
- (g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence;
- (h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and
- (i) provide to the State a detailed plan within 10 calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to

review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination.

21.6 The parties agree that any damages arising out of a breach of the terms set forth in this **Section** are to be considered direct damages and not consequential damages.

22. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication, documentation, materials, information, or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties outside the scope of this Agreement.

22.1 Meaning of Confidential Information. For the purposes of this Contract, the term “**Confidential Information**” means all information, data, materials, reports, plans, manuals, , financials, know-how, methodologies, intellectual property, trade secrets, security, and documentation of a party that: (a) has been marked “confidential” or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked “confidential” or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked “confidential” or with words of similar meaning; and/or, (c) should reasonably be recognized as confidential information of the disclosing party. The term “Confidential Information” does not include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without any obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party’s proprietary rights; (d) obtained from a source other than the disclosing party without any obligation of confidentiality, as known to the receiving party; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

22.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor’s subcontractor is permissible where:

- (a) the subcontractor is a Permitted Subcontractor;
- (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor’s responsibilities; and
- (c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State’s Confidential Information in confidence. At the State’s request, any of the Contractor’s and Permitted Subcontractor’s Representatives may be required to execute a separate agreement to be bound by the provisions of this **Subsection 22.2**.

22.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

22.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

22.5 Surrender of Confidential Information. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 15 Business Days from the date of termination or expiration, return to the other party or destroy any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party’s possession, custody, or control (except to the extent provided in writing under the terms of this Contract or applicable Statement of Work). Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State’s Confidential Information, including State Data, from all media including backups using National Security Agency (“NSA”) and/or National Institute of Standards and Technology (“NIST”) (NIST

Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. If the return of any Confidential Information is not feasible or necessary, Contractor will destroy the Confidential Information as specified above. The Contractor must confirm the destruction of Confidential Information (including State Data) in writing within 15 Business Days from the date of request from the State.

23. Records Maintenance, Inspection, Examination, and Audit.

23.1 Right of Audit. Pursuant to MCL 18.1470, the State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension (“**Financial Audit Period**”). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

23.2 Right of Inspection. Within 10 Business Days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor’s premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract and the Services provided to State, subject to reasonable physical, technical and administrative security procedures of Contractor and at State’s cost. Contractor agrees to cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within 45 calendar days.

23.3 Application. This **Section 23** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

24. Support Services. Contractor will provide the State with the Support Services described in the Service Level Agreement attached as **Schedule D** to this Contract. Such Support Services will be provided:

- (a) Free of charge during the Warranty Period.
- (b) Thereafter, for so long as the State elects to receive Support, in consideration of the State’s payment of Fees for such Services in accordance with the rates set forth in the Pricing Schedule B.

25. Data Security Requirements. Throughout the Term and at all times in connection to the Solution, Contractor will maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State’s Confidential Information that comply with the requirements of the State’s data security policies as set forth in **Schedule E** to this Contract.

26. Training. Contractor will provide, at no additional charge, training on the Solution provided hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State’s request, Contractor will timely provide training for additional Authorized Users or other additional training on the Solution for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

27. Maintenance Releases; New Versions

27.1 Maintenance Releases. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.3 Installation. To the extent applicable, the State has no obligation to install or use any Maintenance Release or New Versions of the Deliverables; however, failure to install required Maintenance Releases or replace expiring Deliverables with New Versions when required to do so, may result in performance failures, to which Contractor shall have no liability regardless of anything to the contrary herein. If the State wishes to install any Maintenance Release or New Version, the State will have the right to have such Maintenance Release or New Version installed, in the State’s discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Accepted Tested by the State. The State’s decision not to install or implement a Maintenance Release (within thirty (30) days of release) or New Version of the Software may affect State’s right to receive Support Services throughout the Term of this Contract.

27.4 Supported Third-Party and Open-Source Components. Contractor will utilize only currently supported versions of all Third-Party or Open Source Components and will notify the State when not using the most recently published Third-Party and Open Source Components.

28. Source Code Escrow

28.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release. The cost of the escrow will be the sole responsibility of Contractor, unless otherwise agreed to in writing.

28.2 Deposit. If applicable where an escrow agreement is signed, within 30 Business Days of the effective date of the escrow agreement, Contractor will deposit with the escrow agent, pursuant to the procedures of the escrow agreement, the Source Code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. Promptly after release of any update, upgrade, patch, bug fix, enhancement, new version, or other revision to the Software, Contractor will deposit updated Source Code, documentation, names, and contact information with the escrow agent (all of which is collectively referred to herein as “**Deposit Material**”).

28.3 Verification. At State’s request and expense, the escrow agent may at any time verify the Deposit Material, including without limitation by compiling Source Code, comparing it to the Software, and reviewing the completeness and accuracy of all material. If the Deposit Material does not conform to the requirements of **Subsection 28.2** above:

- (a) Contractor will promptly deposit conforming Deposit Material; and
- (b) Contractor will pay the escrow agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this **Section 28** will constitute material breach of this Contract, and no further payments will be due from the State until such breach is cured, in addition to any other remedies the State may have.

28.4 Deposit Material License. Contractor hereby grants the State a license to use, reproduce, and create derivative works from the Deposit Material, provided the State may not distribute, sell, or sublicense the Deposit Material or make any use of it whatsoever except for such internal or governmental uses as necessary to maintain and support the Software. Copies of the Deposit Material created or transferred pursuant to this Contract are licensed, not sold, and the State receives no title to or ownership of any copy or of the Deposit Material itself. The Deposit Material constitutes Confidential Information of Contractor pursuant to **Section 22** (Non-disclosure of Confidential Information) of this Contract (provided no provision of **Subsection 22.4** calling for return of Confidential Information before termination of this Contract will apply to the Deposit Material).

29. Contractor Representations and Warranties.

29.1 Authority. Contractor represents and warrants to the State that:

- (a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;
- (b) It has the full right, power, and authority to enter into this Contract, and to perform its contractual obligations;
- (c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and
- (d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms.
- (e) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606.

29.2 Bid Response. Contractor represents and warrants to the State that:

- (a) 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 to the Solicitation; 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;
- (b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor’s Bid Response, 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;
- (c) Contractor 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 within the previous 5 years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

29.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) Contractor is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto or is the recipient of a valid license thereto, and that it has and will maintain the full power and authority to grant a license or use of the Intellectual Property Rights with the Software or to use the Software in the Contract (i) without the further consent of any third party and (ii) without conditions or requirements not set forth in this Contract;

(b) Contractor has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

(c) the Software, and the State's use thereof, is and throughout Term will be free and clear of all encumbrances, liens, and security interests of any kind;

(d) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(e) when used by the State or any Authorized User in accordance with this Contract the Solution as provided, delivered, or installed by Contractor does not or will not:

(i) infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable law;

(f) as provided by Contractor, the Solution does not and will not at any time during the Term contain any:

(i) Harmful Code; or

(ii) Third party or Open Source Components or operate in such a way that it is developed or compiled with or linked to any third-party or Open Source Components, other than Approved Third-Party Components.

(g) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the Term will the Software have any material undocumented feature; and

(h) Contractor will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(i) when used in the Operating Environment and in accordance with the Documentation and applicable Specifications (as may be outlined in a Statement of Work), all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract, the specifications, and the Documentation when used by State for the intended purpose. ;

(j) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever;

(k) no Maintenance Release or New Version, when properly installed (if applicable to State) in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software, to the best of Contractor's knowledge;

(l) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported pursuant to this Contract.

(m) If Contractor Hosted:

(i) Contractor will not advertise through the Solution (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by the State;

(ii) the Solution will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in the Service Level Agreement;

(iii) all Specifications are, and will be continually updated and maintained so that they continue to be, current, complete and accurate and so that they do and will continue to fully describe the Solution in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Solution have any material undocumented feature;

(n) During the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Solution, will apply solely to Contractor or its Permitted Subcontractors, unless signed directly by the State. Regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against State Systems or networks.

29.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS CONTRACT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

30. Conflicts and Ethics. Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value including an offer of employment; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, Affiliate, or subsidiary organization of Contractor, and any Permitted Subcontractor that provides the Solution in connection with this Contract.

31. Compliance with Laws. Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with applicable laws in connection with this Contract.

32. Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, and Executive Directive [2019-09](#), Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

33. Unfair Labor Practice. Under MCL 423.324, the State may void this Contract if the name of the Contractor, or the name of a subcontractor, manufacturer, or supplier of the Contractor, subsequently appears on the Unfair Labor Practice register compiled under MCL 423.322.

34. Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the Michigan Court of Claims. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

35. Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

36. Force Majeure

36.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term

hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, natural disasters, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a “**Force Majeure Event**”), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

36.2 State Performance. In the event of a Force Majeure Event affecting Contractor’s performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. Any date specifically designated for Contractor’s continued performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

36.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions, or malfunctions of the Solution or any of Contractor’s telecommunication or internet services, impacting only Contractor, other than as a result of a general and widespread internet or telecommunications failures that are not limited to the Solution; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

(b) no Force Majeure Event modifies or excuses Contractor’s obligations under **Section 21** (State Data), **22** (Non-Disclosure of Confidential Information), or **17** (Indemnification) of the Contract, Disaster Recovery and Backup requirements set forth in the Service Level Agreement, Availability Requirement (if Contractor Hosted) defined in the Service Level Agreement, or any data retention or security requirements under the Contract.

37. Dispute Resolution. The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties’ respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 Business Days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties’ senior executive and either concludes that resolution is unlikely or fails to respond within 15 Business Days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party decides that a temporary restraining order or other injunctive relief is the only adequate remedy. This section does not limit the State’s right to terminate the Contract.

38. Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

39. Severability. If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

40. Waiver. Failure to enforce any provision of this Contract will not constitute a waiver.

41. Survival. Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification; disclaimer of damages and

limitations of liability; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

42. Administrative Fee and Reporting. Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract for transactions with MiDEAL members and other states (including governmental subdivisions and authorized entities). For clarity, Contractor will not be obligated to pay an additional 1% administrative fee for payments made to the Contractor under the Contract for transactions with the State itself. Administrative fee payments must be made online by check or credit card at: <https://www.thepayplace.com/mi/dtmb/adminfee>. 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. Reports should be mailed to MiDeal@michigan.gov. The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

43. Extended Purchasing Program. This contract is 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 written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees. If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions. Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

44. Contract Modification. This Contract may not be amended or modified in any way, except by a properly signed **Change Notice**. Notwithstanding the foregoing, no subsequent Statement of Work or Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

45. Accessibility Requirements.

45.1 All Software provided by Contractor under this Contract, including associated content and documentation, must at all times conform to the Digital Accessibility Standards. Throughout the Term of the Contract, Contractor must:

- (a) maintain compliance with the Digital Accessibility Standards;
- (b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;
- (c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to the Digital Accessibility Standards;
- (d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor's Software;
- (e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and
- (f) participate in the State of Michigan Digital Standards Review described below.

45.2 State of Michigan Digital Standards Review.

Throughout the Term, Contractor must assist the State, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to review and validate Contractor's accessibility and compliance with the Digital Accessibility Standards. Prior to the Solution going-live a State of Michigan Digital Standards Review is required, and Contractor must remediate all accessibility issues identified in such review at no additional cost.

Additional State of Michigan Digital Standards Reviews may be required thereafter on an annual basis, or as otherwise required by the State. Contractor agrees to remediate any issues identified from any such review pursuant to plans and timelines that are approved in writing by the State.

45.3 Contractor must, without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State arising out of its failure to comply with the foregoing accessibility standards.

45.4 Failure to comply with the requirements in this **Section 45** shall constitute a material breach of this Contract.

46. Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

47. Relationship of the Parties. The relationship between the parties is that of independent contractors. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. Neither party has authority to contract for nor bind the other party in any manner whatsoever.

48. Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

49. No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

50. Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to seek equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy, until or unless required by that court. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this Section.

51. Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and all Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, (or any escrow agreement) and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Deliverables, and the same, if not already in the State's possession or in escrow, if applicable, will be promptly delivered to the State, unless Contractor (or its designee) elects to and does in fact continue to perform all of its obligations under this Contract.

52. Schedules. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing Schedule
Schedule C	Insurance Schedule
Schedule D	Service Level Agreement
Schedule E	Data Security Requirements
Schedule F	Disaster Recovery Plan (if Contractor Hosted)
Schedule G	Transition Plan
Schedule H	Federal Provisions Addendum (if applicable)

53. Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

54. Entire Agreement. These Terms and Conditions, including all Statements of Work and other Schedules and Exhibits (again collectively the "Contract") constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the Terms and Conditions, the Schedules, Exhibits, and a Statement of Work, the following order of precedence governs: (a) first, these Terms and Conditions and (b) second, Schedule E – Data Security Requirements and (c) third, each Statement of Work; and (d) fourth, the remaining Exhibits and Schedules to this Contract. NO TERMS ON CONTRACTOR'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO STATE'S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A – STATEMENT OF WORK

1. DEFINITIONS

The following terms have the meanings set forth below. All initial capitalized terms that are not defined in this Schedule shall have the respective meanings given to them in Section 1 of the Contract Terms and Conditions.

Term	Definition
Offshore Resources	Resources residing outside of the United States, its territories or Canada.
1099	IRS Form 1099-MISC
A/R	Accounts Receivable
AMI	Area Median Income
AR	Annual Re-Examination
B Notice	IRS Backup Withholding Notice
CSV	Comma Separated Values File Type
DHHS	Michigan Department of Health and Human Services
DMS	Document Management System
DPA	Down Payment Assistance
EID	Earned Income Disregard
EIV	Enterprise Income Verification
EOP	End of Participation
FEIN	Federal Employer Identification Number
FMR	Fair Market Rent
FSS	Family Self-Sufficiency
GUI	Graphical User Interface
HAP	Housing Assistance Payment
HCV	Housing Choice Voucher
HO	Homeownership Program
HUD	U.S. Department of Housing and Urban Development
ITSP	Individual Training Service Plan
KTO	MSHDA Key To Own Homeownership Program
MRP	Moderate Rehabilitation Program
MS5	Mainstream Five Program
MSHDA	Michigan State Housing Development Authority
NED	Non-Elderly Disabled Program
PBV	Project Based Voucher Program
PDF	Portable Document Format File Type
PHA	Public Housing Authority
PIC	PIH Information Center
PIH	Public and Indian Housing Office of U.S. Department of Housing and Urban Development
PIP	MSHDA Property Improvement Program
RA	Reasonable Accommodation
RAD	Rental Assistance Demonstration Program

RFTA	Request For Tenancy Approval
SEMAP	Section Eight Management Assessment Program
SQL	Structured Query Language
SSN	Social Security Number
TTP	Total Tenant Payment
UAP	Utility Assistance Payment
VASH	VASH
VMS	Voucher Management System

2. PURPOSE

Contractor will implement, maintain, and support a Contractor-Hosted electronic document management Software Solution and applicable Services for the State's Housing Choice Voucher program to enable the State to move from a paper-driven to digital process. This includes system integration and workflow creation.

3. IT ENVIRONMENT RESPONSIBILITIES

Contractor Hosted Software Solution Definitions:

- **Facilities** – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.
- **Infrastructure** – hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.
- **Platform** – Computing server software components including operating system (OS), middleware (e.g., Java runtime, .NET runtime, integration, etc.), database and other services to host applications.
- **Application** – Software programs which provide functionality for end user and Contractor services.
- **Storage** – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations.
- **Backup** – Storage and services that provide online and offline redundant copies of software and data.
- **Development** - Process of creating, testing and maintaining software components.

Component	Contractor(s) and/or subcontractor(s) providing each contract component
Facilities	Microsoft
Infrastructure	Microsoft
Platform	Microsoft
Application	Hyland Software
Storage	Microsoft
Backup	Microsoft
Development	Hyland Software

4. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with the Digital Accessibility Standards.

5. USER TYPE AND CAPACITY

Contractor Solution must meet the expected number of concurrent Users below:

Type of User	Access Type	Number of Users	Number of Concurrent Users
State Employees: MSHDA Staff	Read/Write	60	60
State Employees: MSHDA Technical Support Services Staff	App Admin	10	10

MSHDA Contracted Partners	Read/Write	250	200
---------------------------	------------	-----	-----

6. ACCESS CONTROL AND AUTHENTICATION

The Contractor's Solution must implement identity federation with the State's MiLogin IT Identity and Access Management (IAM) environment as described in the State of Michigan Administrative Guide ([1340.00.020.08 Enterprise Identity and Access Management Services Standard \(michigan.gov\)](#)).

To support federation with the SOM MiLogin solution, the Contractor's solution must support SAML, OpenID or OAuth federated identity protocols. Solutions running within the State's internally managed IT environment may be suitable for integration with the State's Active Directory services as identified in the 1340.00.020.08 standard.

7. DATA RETENTION AND REMOVAL

The Solution allows the State to retain State Data and User Data for the Term of the Contract. The Solution allows the State to delete data, even data that may be stored off-line or in backups. The Solution allows the State to retrieve data, even data that may be stored off-line or in backups.

8. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes FedRAMP authorized major cloud providers and on-premises market leading virtualization environments, with supporting platforms that includes enterprise storage, monitoring, and management running in house and in cloud hosting provides.

Contractor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users are able to access online services, Contractor must ensure applications and websites display and function accurately in, at minimum, the two most recent major versions of the following browsers, without reliance on special plugins or extensions:

- Google Chrome
- Microsoft Edge
- Firefox
- Safari

Contractor must support the current and future State standard environment at no additional cost to the State.

9. SOFTWARE

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet**. Contractor must provide a Software Bill of Materials (SBOM) containing details and supply chain relationships of various components used in the Solution. The SBOM will contain all open source and third-party components, libraries, and dependencies included with or used in connection with the Solution. This information must be provided to the State in a mutually agreed format on a quarterly basis and for new components at 30 calendar days prior to being added to the Solution.

Look and Feel Standards

All Software items provided by the Contractor must adhere to the State of Michigan Application/Site standards which can be found at <https://www.michigan.gov/standards>.

Mobile Responsiveness

If the Software will be used on a mobile device as define in Schedule A – Table 1, Business Specification Worksheet, the Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

10. INTEGRATION

Contractor must integrate their Solution to the following technologies:

Current Technology	Emphasys Elite
Volume of Data	Unknown at this time
Format of the input & export files	Varies
<p>The Solution must integrate in with MSHDA's Emphasys Elite system so the provided Solution will pull and display record information from Emphasys. Also, if a record exists in Emphasys Elite, it is expected to have a corresponding folder in OnBase for the electronic files. Additionally, we would want to be able to easily access OnBase Information from a currently selected Elite Record.</p> <p>Data lookups will be configured to pull data from Emphasys Elite for indexing in OnBase. The OnBase Application Enabler module will also be used to enable document and folder retrieval directly from Emphasys Elite screens.</p>	

11. MIGRATION

Data migration services are not needed at this time.

12. TRAINING SERVICES

The Contractor must provide online administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency. Contractor will provide online training for up to 80 State internal staff users, 10 of whom would be administrative users. Contractor will also provide such training materials as would enable the State to train external public citizen users. i3-ImageSoft will provide the following training courses:

Solution Training Classes - Train-the-Trainer Methodology	# of Sessions
Includes both preparation time and training for up to ten (10) people in each training below.	
OnBase Functional and Scan Training (Unity Client)	2
OnBase Business Automation Training - Workflow	2
Conduct TrueSign Functional Training	2
Conduct System Administrator Solution Knowledge Transfer	2

These trainings can be either in-person or remote. Remote trainings may be recorded to share with more individuals.

13. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software, collectively as part of the Documentation. Contractor must develop and submit for State approval complete, accurate, and timely Solution documentation to support all users, and will update any discrepancies, or errors through the Term of the Contract. The Contractor's user Documentation must provide detailed information about all Software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests.

14. CONTRACTOR PERSONNEL

Key Personnel:

Contractor Project Manager. Contractor resource who is responsible to serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation Services, matters pertaining to the receipt and processing of support requests and the Support Services.

Tim Zarzycki 403 S. Main St., Royal Oak, MI 48067 586-942-8423 tzarzycki@i3verticals.com

Contractor Security Officer. Contractor resource who is responsible to respond to State inquiries regarding the security of the Contractor's Solution. This person must have sufficient knowledge of the security of the Contractor Solution and the authority to act on behalf of Contractor in matters pertaining thereto. Contractor must inform the State of any change to this resource.

Neil Watkins 40 Burton Hills Blvd., Suite 415, Nashville, TN 37215 615-656-4755 neil.watkins@i3verticals.com

Non-Key Personnel:

Contractor Contract Administrator. Contractor resource who is responsible to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Crystal Bell 403 S. Main St., Royal Oak, MI 48067 262-498-6513 crystal.bell@i3verticals.com
--

15. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks. Contractor agrees to present confirmations evidencing satisfactory ICHAT and drug test results for Contractor Personnel identified for assignment to this project to the State of Michigan Program Manager designated for this Contract. In addition, proposed Contractor Personnel will be required to complete a Michigan State Police background check and/or submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC), if required by project.

Annually, Contractor must perform an ICHAT for Contractor Personnel identified for assignment to this project. Annual background check results will be reported to the State of Michigan Program Manager designated for this Contract.

Contractor, while employed with DTMB, will disclose to the State of Michigan Program Manager for this Contract, in writing at or before the beginning of the next scheduled duty shift:

- a. A felony or misdemeanor court conviction, whether by guilty plea, no contest plea or trial.
- b. A felony arraignment.
- c. Restriction, suspension, or loss of driving privileges for any reason, if the employee's current position requires possession of a valid driver's license.

Contractor will pay for any costs associated with ensuring Contractor Personnel meet applicable requirements.

In accordance with the terms of the Contract, Contractor will notify the State Program Manager(s) prior to removing or replacing any Contractor Personnel with access to State Data under this Contract. Contractor must also provide written confirmation to the State Program Manager(s) that Contractor Personnel's access to State Data has been terminated. Contractor will notify the State thirty (30) days in advance of allocating Contractor Personnel to multiple State Contracts or Projects. Contractor will provide detail of how a given Contractor Personnel meets the resource experience requirements in advance of replacing a Contractor Personnel. Upon request by State and subject to confidentiality obligations, the Contractor will provide a summary of applicable Contractor Personnel who have access to State Data and allocation of time.

Pursuant to the terms of the Contract, Contractor will notify the State prior to removing or replacing any Contractor Personnel with access to State Data.

Offshore Resources. Use of Offshore Resources is prohibited per the Schedule E – Data Security Requirements. Contractor must comply with the data security and other requirements in this Contract.

Disclosure of Subcontractors. If the Contractor intends to utilize subcontractors, the Contractor will provide and disclose the following:

- The legal business name; address; telephone number; a description of subcontractor's organization and the Services it will provide; and information concerning subcontractor's ability to provide the Contract Services.
- The relationship of the subcontractor to the Contractor.
- Whether the Contractor has a previous working experience with the subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Contract Services that will be performed or provided by the subcontractor, who becomes a Permitted Subcontractor.
- If the parties agree, they may add requested subcontractor as a Permitted Subcontractor by executing a Contract Change Notice.

Permitted Subcontractors

The following organizations will be Permitted Subcontractors:

- Microsoft Corporation will provide hosting, storage and backup.
- Hyland Software will provide the application development and maintenance and second level support for matters Contractor cannot resolve without assistance.

16. STATE RESOURCES

The State will provide the following resources as part of the implementation and ongoing support of the Solution. In addition to the resources identified below, the State will make other resources, systems, and information reasonably available for Contractor to meet the Milestone Dates and obligations of this Statement of Work.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Contract Administrator
Jarrold Barron 517-249-0406 BarronJ1@michigan.gov

Program Managers. The DTMB and Agency Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

DTMB Program Manager
Michael Weiszbrod 517-242-1272 WeiszbrodM@michigan.gov

Agency Program Manager
Mark Whitaker 517-420-4878 WhitakerM@michigan.gov

17. MEETINGS

The Contractor will attend the following meetings at no additional cost to the State:

At start of the engagement, the Contractor Project Manager must facilitate a project kick off meeting with the support from the State’s Project Manager and the identified State resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, Contractor Project Manager will facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor will facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

18. PROJECT CONTROL & REPORTS

Once the Project Kick-Off meeting has occurred, the Contractor Project Manager will monitor project implementation progress and report on a weekly basis to the State’s Project Manager the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period
- Indicate the number of hours expended during the past week, and the cumulative total to date for the project. Also, state whether the remaining hours are sufficient to complete the project
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified
- Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

19. PROJECT MANAGEMENT

The Contractor Project Manager will be responsible for maintaining a project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources – both Contractor and State - required to meet the timeframes as agreed to by both parties. Changes to scope, schedule or cost must be addressed through a formal change request process with the State and the Contractor to ensure understanding, agreement and approval of authorized parties to the change and clearly identify the impact to the overall project.

SUITE Documentation

In managing its obligation to meet the above milestones and deliverables, the Contractor is required to utilize the applicable [State Unified Information Technology Environment \(SUITE\)](#) methodologies, or an equivalent methodology proposed by the Contractor.

Milestones/Deliverables for Implementation

The parties agree to the preliminary milestone schedule and associated deliverables are set forth below. A detailed project plan would be created as part of the Project Planning milestone. The Parties would agree to the schedule within this Project plan.

Milestone Event	Associated Milestone Deliverable(s)	Schedule
Project Planning	Project Kickoff	Contract Execution + twenty (20) Business Days

Requirements and Design Validation	Validation sessions, Final Requirement Validation Document, Final Design Document, Final Implementation Document	Execution + 90 calendar days
Provision environments	Validate Test and Production environments	Execution + 90 calendar days
Installation and Configuration of software	Final Solution and Testing Document	Execution + 120 calendar days
Testing and Acceptance	Final Test Results Report, Final Training Documentation, State of Michigan Digital Standards Review and Approval, Final Acceptance	Execution+150 calendar days
Post Production Warranty	Included in the cost of Solution.	Production + 90 calendar days
Production Support Services	Ongoing after Final Acceptance.	Ongoing

20. ADDITIONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract, subject to Contractor’s approval and such will be documented in writing and signed as a Contract Change Notice by an authorized representative of both parties.

SCHEDULE A, ATTACHMENT 1 – BUSINESS SPECIFICATION WORKSHEET

Contractor will meet each business Specification as stated herein.

The Business Specifications Worksheet contains columns and is defined as follows:

Column A: Business Specification number.

Column B: Business Specification description.

Column C: Indicates how Contractor will comply with the business Specification.

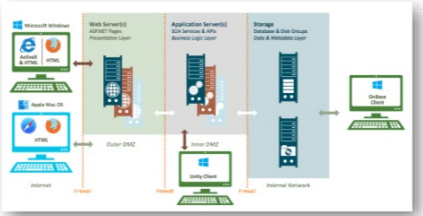
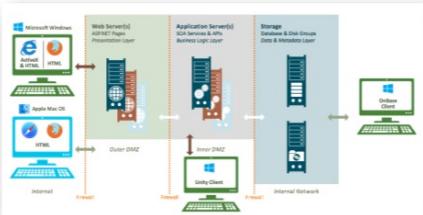
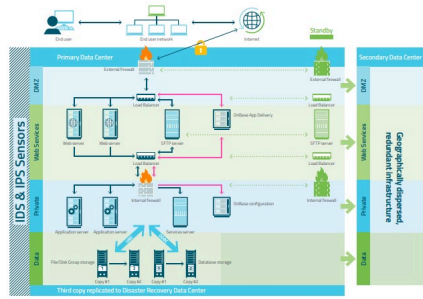
- **Current Capability** – This capability is available in the proposed Solution with no additional configuration or cost.
 - **Requires Configuration** – This capability can be met through Contractor-supported changes to existing settings and application options as part of the initial implementation at no additional cost (e.g., setting naming conventions, creating user-defined fields). Configuration is referred to as a change to the Solution that must be completed by the awarded Contractor prior to Go-Live but allows an IT or non-IT end user to maintain or modify thereafter (i.e. no source code or structural data model changes occurring).
 - **Customizations to Software Required** – The requirement can be met through Contractor modifying the underlying source code, which can be completed as part of the initial implementation. Customization is referred to a modification to the Solution's underlying source code, which can be completed as part of the initial implementation.
 - **Future Enhancement** – This capability is a planned enhancement to the base software and will be available within the next 12 months of contract execution at no additional cost.
 - **Not Available** – This capability is not currently available, and a future enhancement is not planned.
- configuration changes or customization modifications made during the term of the awarded contract must be forward-compatible with future releases and be fully supported by the awarded Contractor without additional costs.

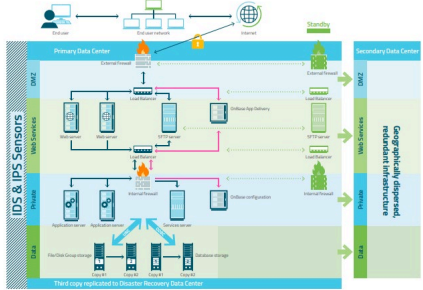
Column D: Details how the Contractor will deliver each Business Specification and if the Contractor proposes configurations or customizations, explains the details of the impacted risk that may be caused if configured or customized to meet the Business Specification.

A	B	C					D
Business Specification Number	Business Specification	Current Capability	Requires Configuration	Requires Customization	Future Enhancement	Not Available	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
1. (2.1)	The System must support 300-500 logged in users both internally and externally simultaneously	Y					There is no system limitation to the number of users that can access the system.

2. (2.2)	The system must support a user role-based security solution that allows role-based access to screens, buttons, functions and reports (e.g., no access, read only, update).	Y				Unique levels of security are achieved by creating a custom set of product rights and privileges for each OnBase user group. After the OnBase System Administrator has created a user group structure, individual users are made members of one or more user groups. If a user is a member of multiple user groups, the user is granted the cumulative rights of all the member groups. An OnBase administrator can rapidly implement a custom security profile for each user or group of users within an enterprise. Users can be added/deleted using an intuitive point-and-click GUI in the OnBase Configuration module. Likewise, the set of product rights and privileges defined for each user group can be modified as easily.
3. (2.3)	The system must support a process for system administrators to approve system access to any user or role.	Y				The security model used in the OnBase system provides for the segregation of data between users, as well as the ability to limit the product functionality available for each user. User Groups and Rights provides for the assignment or restriction of basic and advanced OnBase features. Privileges can be assigned in an extremely granular manner in OnBase. This includes securing applications, document types, folders, and features like the ability to edit. Users can also be given read only rights to specific keyword types, or the keyword values themselves can be hidden. Indexing Limits can also be assigned to a user group, in order to limit a user's ability to index documents with specific keyword values.
4. (2.4)	The system must have a function for an administrator role to approve system access to new users.	Y				Administrators can create user accounts directly, map accounts from Active Directory or other authentication

							system, or approve self-registered accounts.
5. (2.5)	The system must allow the creation, edit and deletion of user accounts.	Y					Authorized Admins can create, edit, lock/unlock, and delete user accounts.
6. (5.6)	The system must allow administrators to set data retention schedules as required by the organization	Y					OnBase Records Management controls the retention of all associated business records securely organized within the OnBase Folders interface. The retention cycle of a folder is triggered by an event (or the passage of time), which ties records management strategies into organizational business processes. The module provides cutoff periods, retention plans, multiple destruction options, and offers the ability to apply legal holds. OnBase Records Management also offers exception handling as well as an administrative management interface.
7. (5.7)	The system must have the ability to purge records based on retention schedule.	Y					Records can be automatically purged based on retention schedules or sent for review/approval before purging of records.
8. (8.1)	Have system training on Workflow and reporting	Y					Training is provided for all aspects of the solution including workflow and reporting.
9. (8.2)	Vendor must provide user manual	Y					User manuals are provided as part of the end user training.
10. (8.3)	Vendor must provide Security/Privileged user training	Y					Administrator training is provided.
Integration							
11. (10.1)	The system must be able to integrate with Emphasys Elite.	Y					Data lookups will be configured to pull data from Emphasys Elite for indexing in OnBase. The OnBase Application Enabler module will also be used to enable document and folder retrieval directly from Emphasys Elite screens.
Documentation and Standards							

12. (11.1)	Provide a logical network diagram that describes how the infrastructure components will meet the functional requirements	Y				
13. (11.2)	Provide conceptual and logical data-flow diagrams	Y				
14. (11.3)	Provide a high-level architecture diagram, including logical and physical components	Y				
15. (11.4)	The system must support a Recovery Point Objective as agreed per MSHDA	Y				i3-ImageSoft can support the Recovery Point Objective as defined in Section 6.4 of Schedule D – Service Level Agreement (Contractor Hosted)
16. (11.5)	The system must support a Recovery Time Objective As Agreed per MSHDA	Y				i3-ImageSoft can support the Recovery Time Objective as defined in Section 6.4 of Schedule D – Service Level Agreement (Contractor Hosted)
17. (11.6)	System documentation must describe required application maintenance activities and time frames	Y				i3-ImageSoft will provide updates/release notes for required application maintenance activities and timeframes for OnBase. Any Microsoft updates would be provided via the Microsoft website.
18. (11.8)	Provide a continuity of business and disaster recovery plan	Y				As part of the Project a business and disaster recovery plan will be developed

Application Security							
19. (13.1)	If awarded a contract, the vendor must successfully participate in the DTMB System Security Plan process prior to implementing the solution to production.	Y					i3-ImageSoft will participate in the DTMB System Security Plan process prior to implementing the solution to production
20. (13.2)	The solution must have built-in security controls and meet or exceed current SOM security requirements. The SOM will base its IT governance framework on Control Objectives for Information Technologies (COBIT) (https://www.isaca.org/resources/cobit) and will select its IT security controls from and National Institute of Standards and Technology (NIST) (http://www.nist.gov/information-technology-portal.cfm) SP 800-53.	Y					i3-ImageSoft hosted environment will comply with this requirement
21. (13.4)	Client application must support encryption of data both at rest and in transit, in accordance with the data classification	Y					OnBase can support encryption of data both at rest and in transit.
Identity Management							
22. (15.1)	A detailed network/server diagram must be provided illustrating the relative architecture of the proposed system. It should include: Ports and protocols used to cross security zones How users will access the system	Y					
23. (15.2)	the vendor will participate with the State to obtain an approved Enterprise Architecture (EA) Solution Assessment, prior to production.	Y					i3-ImageSoft will participate to obtain approved Enterprise Architecture Solution prior to implementing the solution to production
System Administration and Licensing							
24. (16.1)	Software licensing must be inclusive for all packages included in the solution, unless explicitly listed and detailed	Y					The proposed solution includes all the software licensing needed for the

							system. No additional third-party licensing is required.
25. (16.4)	All known security vulnerabilities must be addressed in accordance with industry-accepted system hardening standards. Industry-accepted standards include: Sysadmin Audit Network Security (SANS) Center for Internet Security (CIS) SOM DTMB Standards	Y					i3-ImageSoft hosted environment will comply with this requirement
26. (16.5)	Prevention of common coding vulnerabilities must be covered in software development processes, including: a)Cross-side scripting (XSS) b)Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws. c)Malicious file execution d)Unsecure direct object references e)Cross-site request forgery (CSRF) f)Information leakage and improper error handling g)Broken authentication and session management h)Unsecure cryptographic storage i)Unsecure communications j)Failure to restrict URL access	Y					OnBase supports best practices during the software development process to prevent common coding vulnerabilities.
Application Design							
27. (17.1)	Applications and systems must conform with SOM eMichigan Policy regarding "Look and Feel Standards for Web applications and Sites": https://www.michigan.gov/standards	Y					Both the Web Client and Web App Builder have configurable options and allow for site branding. Custom portal interfaces can also be built that give complete control over the user experience including the look, feel, and functionality.
28. (17.2)	Americans with Disabilities Act (ADA) compliant		Y				The Web Portal components of the solution are designed with ADA compliance standards. This includes things like panel layouts, device responsiveness, color choices, screen reader accessibility, etc. A Published

							Voluntary Product Accessibility Template (VPAT) is also available upon request.
Document Intake							
29. (1.1)	The System must have configurable Categories (Example: Entity Type - e.g. landlord files, resident files...)	Y					OnBase uses the concept of document types that can be assigned to document type groups. Document type groups represent a logical grouping of document types in the database. Each document type can also have its own set of index fields called Keywords. OnBase Folders can also be used to organize documents into logical grouping
30. (1.2)	The System must have configurable name conventions	Y					Naming conventions are configurable. OnBase supports using auto name strings for document names. Auto name strings can include index information, document properties, and/or static values.
31. (1.3)	The system must have configurable file structure (replicate paper file)	Y					OnBase Folders provide a familiar interface for grouping documents without changing their physical storage in the database or association to a document type. Displaying documents in a hierarchy is best obtained using the File Cabinets and Folders feature of OnBase. Documents can be placed dynamically into a folder during a scanning or import process. Documents can also be placed in an open folder by drag-and-drop. A document can exist in more than one folder at the same time, because the folder contains pointers to the document rather than actual copies of the documents. The manner in which documents are placed into folders is typically driven by common keyword criteria.
32. (1.4)	The system must have configurable metadata	Y					Metadata/Keywords can support all types of information and there is no limit

							to the number of Keywords that can be used.
33. (1.5)	The system must have configurable quality and file size for both documents and photos	Y					OnBase stores all documents in their native format and does not use any proprietary formatting, image headers, or compression. OnBase does not pose any restrictions to the file formats that can be stored and can natively view most file formats within the standard OnBase viewer.
34. (1.6)	The system must have configurable automated behaviors	Y					OnBase Workflow can be used to evaluate business rules and execute actions without user intervention.
35. (1.7)	The system must have configurable document workflows	Y					OnBase Workflow is a rules-based electronic document routing system that enables users to process work more efficiently, faster, and more accurately than with traditional paper processing. With OnBase Workflow, users or integrators define and configure document states, rules, actions, and Life Cycles with a graphical Windows interface. Upon configuration, Workflow instantly routes documents through the business process as each increment of user or system work is completed. Standard features include routing, approvals, notifications, system work, and timers. OnBase Workflow also supports such advanced features as alternate routing logic, automatic criteria calculation, rendezvous, simultaneous notification, load balancing, reporting, Ad Hoc Workflow, Scripting, and API functionality for integration with other systems.
36. (1.8)	The system must have the ability to upload files or scan documents directly into the system	Y					Importing content into the OnBase repository can be accomplished in a variety of different methods, including the following:

							<ul style="list-style-type: none"> • Document Imaging - Scans, indexes and stores documents as digital images. • COLD/ERM Processing - Automatically indexes and stores reports and statements that are output from computer systems as printer, COM or text files. • PDF Input Filter to COLD/ERM - This allows PDFs to automatically be brought into OnBase, separated into multiple documents (if need be), and indexed from metadata contained within the file. • Document Import Processor (DIP) - Imports batches of documents and auto-indexes them based on a metadata file. • Directory Import Processor - Imports documents utilizing file and folder names for keyword information. • Ad hoc Document Import - Allows a user to drag and drop or scan a single document. • API Archival - Allows for the storage of documents from third party systems into the OnBase system via the OnBase API. • Electronic Forms - Enables users to complete and submit online forms that are automatically captured, indexed, and stored as documents in OnBase. <p>Mailbox Importer - Automatically imports email messages and attachments by polling email accounts.</p>
--	--	--	--	--	--	--	--

37. (1.9)	The system must allow the user based on role to manually enter metadata during document upload	Y					Metadata can be entered during upload or later through a re-index option.
38. (1.1)	The system must employ data validation techniques on required data field on documents.	Y					OnBase offers multiple field validation features including type, length, choice lists, masking, and required fields. OnBase also supports field validation against external systems or databases.
39. (1.11)	The system must provide ability to transform existing and new forms/file types to digitally fillable forms	Y					OnBase supports EForms and includes a Forms Designer tool.
Document Management							
40. (3.1)	The system must allow a user based on role to delete, move, and rename files	Y					The ability to delete, move, or rename a file is a permission that can be granted to specific users, groups, or roles.
41. (3.2)	The system must allow a user based on role to add, edit and delete metadata.	Y					The ability to add, edit, or delete metadata is a permission that can be granted to specific users, groups, or roles.
42. (3.3)	The system must allow a user based on role to configure document templates	Y					The ability to create and modify document templates is a permission that can be granted to specific users, groups, or roles.
43. (3.4)	Utilized download and store files in a non proprietary common format, this would include keeping file in the same format that it was uploaded in when downloading the file.	Y					OnBase stores all documents in their native format and does not use any proprietary formatting, image headers, or compression. Authorized users can export files from the OnBase system as needed.
44. (3.5)	The system must have the ability to automatically extract metadata for use in indexing and routing documents within the system.	Y					OnBase provides an Advanced Capture Module that can be used to classify and extract metadata from newly imported documents.
45. (3.6)	The system must allow for a document batch to be uploaded or scanned to be reviewed, indexed, separated, and assigned to individual records within system.	Y					OnBase includes scanning capabilities as well as capture process flows where steps can be used for separation, indexing, and quality assurance reviews.

46. (3.7)	The system must create and maintain a history of modified documents with the ability to restore a document to a previous version.	Y					OnBase provides a complete document history log for every document in the system. This log tracks the date and time, the user, and the action performed. In addition to the document history, OnBase also tracks each workflow queue a document has been in and who worked the document in and out of that queue. Furthermore, workflow task execution can be enabled to log details of specific workflow actions if desired.
47. (3.8)	The system must allow a user based on role to recover documents deleted in error.	Y					OnBase uses a Recycle Bin concept where authorized admins can restore deleted files.
48. (3.9)	The system must allow users to search for documents including but not limited to, *File Name *Metadata *OCR Search	Y					OnBase provides multiple searching options including Document Retrieval, Custom Queries, Folder Searching, and Workflow Filtering. Content can be retrieved by using keywords, date ranges, operators, note text, and/or by full text searching. OnBase Full-Text Search provides a simple, unified interface for retrieving textual information stored in OnBase documents. This module extends native OnBase search capabilities to both structured and unstructured data. Advanced searches, such as fuzzy, thesaurus, near, soundex, and wildcard can be used as well as boolean operators (e.g. and, not, or) to quickly and accurately locate specific documents
49. (3.10)	The file structure must automatically be created and incorporate all necessary folders to house needed electronic files for the HCV Program.	Y					OnBase Folders provide a familiar interface for grouping documents without changing their physical storage in the database or association to a document type. Displaying documents in a hierarchy is best obtained using the File Cabinets and Folders feature of OnBase. Documents can be placed

							dynamically into a folder during a scanning or import process. Documents can also be placed in an open folder by drag-and-drop. A document can exist in more than one folder at the same time, because the folder contains pointers to the document rather than actual copies of the documents. The manner in which documents are placed into folders is typically driven by common keyword criteria.
50. (3.11)	The system must allow individual files to be bundled together where all documents that were linked can be viewed together in a specific order.	Y					OnBase supports dynamic, content sensitive, document linking capabilities via cross-referencing. OnBase cross-referencing provides the ability to link documents based on like values. Documents can be linked across a single application or different applications, as long as there is a common index value. Static cross-referencing is also available by "stapling" documents together via a drag-and-drop, or accumulating documents into an envelope.
Workflow							
51. (4.1)	The system must allow a user based on role to manage the workflow	Y					Workflow admins can be designated to create and/or manage workflow processes.
52. (4.2)	The system must allow for single documents to have a configuration of document workflows	Y					Individual documents can be entered into workflow processes as well as eForms, Folders, and Data Objects.
53. (4.3)	The system must allow for group of documents to have a configuration of document workflows	Y					Individual documents can be entered into workflow processes as well as eForms, Folders, and Data Objects.
54. (4.4)	The system must allow for documents to be sent via email for review, complete and digitally sign.	Y					Documents can be emailed from the system as well as sent through TrueSign to acquire signatures.
55. (4.5)	The system must provide configurable parameters to remind recipients of outstanding documents requiring attention.	Y					Notifications and reminders are a native component to workflow. Notifications can be configured on when

							they are sent and what content is included in the notification message.
56. (4.6)	The system must provide notification/alerts when a task has been completed in a document workflow	Y					Notifications and reminders are a native component to workflow. Notifications can be configured on when they are sent and what content is included in the notification message.
57. (4.7)	The system must provide a workflow for 250 - 300 external contracted partners to do HCV recertifications and include internal MSHDA staff for necessary approvals	Y					Workflows can be created for any number of participants including external partners.
58. (4.8)	The system must allow HCV staff to review external partners workflow statuses for HCV recertifications.	Y					Any content submitted by external participants can be sent for review by internal HCV Staff.
59. (4.9)	The system must have or be configured with the following workflows 1. Eligibility – This workflow will gather information from a selected applicant, route the documentation for review and eligibility determination. (250-300 external partners to initiate workflow) 2. Lease-Up – This workflow will be used to gather and route documents for signature and approval during the lease-up process. (250-300 external partners + possible MSHDA staff) 3. Annual Reexamination – This workflow will gather annual documentation on certification of a participant’s household, income, assets, etc. (250-300 external partners + possible MSHDA staff) 4. Interim Reexamination – This workflow will gather documents and information regarding applicable changes to a participants voucher case. (this is abbreviated from the larger Annual Reexamination) (250-300 external partners + possible MSHDA staff) 5. Hearings – This workflow will route a request for hearing through each step of	Y					The proposed solution includes workflows for all of these processes.

	remediation to the final determination. Final determination needs to go back to external partner. (250-300 external partners + possible MSHDA staff)						
Audit							
61. (5.1)	The system must support record auditing including the date/time a record is created, who created the record, the date/time a record is modified and who modified the record.	Y					OnBase provides a complete document history log for every document in the system. This log tracks the date and time, the user, and the action performed. In addition to the document history, OnBase also tracks each workflow queue a document has been in and who worked the document in and out of that queue. Furthermore, workflow task execution can be enabled to log details of specific workflow actions if desired.
61. (5.2)	Changes to user access permissions must be loggable and have audit trail(s) which can be provided to MSHDA upon request or are accessible to system administrators	Y					Administrative changes are logged and can be reported on as needed.
62. (5.3)	Access to audit trail logs must be able to be restricted to approved administrators	Y					The ability to see audit information or run transaction reports is a privilege that can be granted to select users only.

63. (5.3)	Access to Document audit trail logs must be able to restricted to appropriate role.	Y					The ability to see audit information is a privilege that can be granted to select user groups or roles.
64. (5.4)	The system must provide a full audit of all workflow notifications, including the state of a record before and after a change, who sent the notification, who received the notification, and the mechanism used to send the notification.	Y					The sending of notifications can be tracked and added to the audit log. The actual notification itself can also be archived in OnBase for audit purposes.
65. (5.5)	Provide ability to perform monitoring/auditing as required by the State and Federal standards	Y					OnBase provides multiple monitoring and auditing tools.
66. (5.8)	Ability to generate reports of active/inactive application users	Y					OnBase has the ability to monitor user activity and an area to view active users. Reports can also be ran for things like last log on and failed attempts.
67. (5.9)	System must provide a last user login date	Y					Last log on date and time is tracked and can be viewed by authorized admins.
68. (5.1)	System/Vendor alert appropriate security and incident personnel upon detection of unauthorized access, modification, or deletion of audit information.	Y					Alerts can be sent based on a number of criteria including unauthorized access and failed attempts.
69. (5.11)	Systems provide record generation capability for the following types of events at the database and the application layer: User account management activities, Database shutdown, Database restart, Database errors, Failed and successful log-ons, Security policy/configuration modifications, Use of administrator commands, Change of password, Changes to database records, Security policy/configuration modifications, Change of application critical records.	Y					All of these events are recorded and can be used in reporting.
70. (5.12)	The system must create and maintain a history of modified documents with the ability to restore a document to a previous version.	Y					Audit information is retained for all documents in the system
System Notifications							
71. (6.1)	The system must have alerts and reminders of outstanding tasks, follow ups, etc. for users	Y					Email notifications are natively supported with workflow. Notifications can be sent automatically when items

							are assigned, when certain statuses are present, or based on user actions. Notifications can also be used for alerting users of time sensitive work items, missed SLA's, or as part of an escalation process.
72. (6.2)	The system must produce post notification	Y					Email notifications are natively supported with workflow. Notifications can be sent automatically when items are assigned, when certain statuses are present, or based on user actions. Notifications can also be used for alerting users of time sensitive work items, missed SLA's, or as part of an escalation process.
73. (6.3)	The system must have a notification system that alerts users of tasks that have been assigned to them.	Y					Email notifications are natively supported with workflow. Notifications can be sent automatically when items are assigned, when certain statuses are present, or based on user actions. Notifications can also be used for alerting users of time sensitive work items, missed SLA's, or as part of an escalation process.
Reporting Functionality							
74. (7.1)	The system must allow for Ad Hoc reporting based on role	Y					OnBase offers standard reports that authorized users can run directly from the OnBase client. These include configuration, exception, transaction, and verification reports. OnBase also offers a Reporting Dashboards Module which allows users to create graphical views based on relevant information. Dashboards present data in a variety of graphical formats including charts, graphs, scorecards, maps and more. Interactive features then allow users to easily monitor performance and analyze trends in real-time.
Technical							

Client/Workstation

75. (9.1)	The solution must be compatible with different operating systems which must comply with current DTMB version standards.	Y				<p>OnBase includes multiple client options including a browser-based Web Client, a ribbon bar Windows Style Client, and a Mobile Client.</p> <table border="1" data-bbox="1497 329 1923 743"> <thead> <tr> <th>Operating System</th> <th>Client</th> <th>Web/Application Server</th> <th>Web Client</th> <th>Unity Client</th> </tr> </thead> <tbody> <tr> <td>Windows 10</td> <td>X</td> <td>N/A</td> <td>X</td> <td>X</td> </tr> <tr> <td>Windows Server 2019</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Windows Server 2019 Server Core</td> <td>N/A</td> <td>X</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td>Windows 11</td> <td>X</td> <td>N/A</td> <td>X</td> <td>X</td> </tr> <tr> <td>Windows Server 2022</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Windows Server 2022 Server Core</td> <td>N/A</td> <td>X</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td>Apple macOS (Version 12 or later version)</td> <td>N/A</td> <td>N/A</td> <td>X</td> <td>N/A</td> </tr> </tbody> </table>	Operating System	Client	Web/Application Server	Web Client	Unity Client	Windows 10	X	N/A	X	X	Windows Server 2019	X	X	X	X	Windows Server 2019 Server Core	N/A	X	N/A	N/A	Windows 11	X	N/A	X	X	Windows Server 2022	X	X	X	X	Windows Server 2022 Server Core	N/A	X	N/A	N/A	Apple macOS (Version 12 or later version)	N/A	N/A	X	N/A
Operating System	Client	Web/Application Server	Web Client	Unity Client																																										
Windows 10	X	N/A	X	X																																										
Windows Server 2019	X	X	X	X																																										
Windows Server 2019 Server Core	N/A	X	N/A	N/A																																										
Windows 11	X	N/A	X	X																																										
Windows Server 2022	X	X	X	X																																										
Windows Server 2022 Server Core	N/A	X	N/A	N/A																																										
Apple macOS (Version 12 or later version)	N/A	N/A	X	N/A																																										
76. (9.2)	The solution must be compatible with all SOM supported internet browsers which must comply with current DTMB version standards.	Y				The Web Client is supported on standard browsers like Chrome, Edge, Firefox, and Safari.																																								
77. (9.3)	The solution must be compatible with multiple hardware platforms (e.g. mobile phone, laptop, tablet, etc.) which must comply with current DTMB version standards.	Y				OnBase includes multiple client options including a browser-based Web Client, a ribbon bar Windows Style Client, and a Mobile Client. OnBase also includes a Web App Builder to create client interfaces based on specific user types or roles. This allows for a browser-based experience that is more streamlined and simplified.																																								
78. (9.4)	The system must be compatible with non-proprietary consumer available scanning and imaging equipment.	Y				<p>OnBase includes multiple scanning options including ad hoc scanning, batch scanning, and web scanning. OnBase is hardware independent and supports any TWAIN, ISIS, or Kofax™ compliant scanning device. Multifunction devices can also be utilized to scan to a network folder or email that OnBase monitors and ingests on a regular basis.</p>																																								

79. (9.5)	The system must be able to view documents without downloading each file.	Y					Documents can be viewed directly within the OnBase Clients.
80. (9.6)	The system must allow external recipients to review, complete, and digitally sign a document or group of documents without the need to download the documents or additional software.	Y					TrueSign will allow external signers the ability to view and sign documents from a standard web browser.
Integration							
81. (10.2)	The system must be able to view and retrieve documents from open records in Elite without needing to complete another search within the system	Y					OnBase Application Enabler will allow retrieval of OnBase Documents directly from Elite screens.
82. (10.3)	The system must create a new set of standard folder set when a new record in Elite is created	Y					OnBase Folders provide a familiar interface for grouping documents without changing their physical storage in the database or association to a document type. Displaying documents in a hierarchy is best obtained using the File Cabinets and Folders feature of OnBase. Documents can be placed dynamically into a folder during a scanning or import process. Documents can also be placed in an open folder by drag-and-drop. A document can exist in more than one folder at the same time, because the folder contains pointers to the document rather than actual copies of the documents. The manner in which documents are placed into folders is typically driven by common keyword criteria.
83. (10.4)	The system must pull data from Emphasys Elite in real time	Y					OnBase supports data lookups from external systems like Elite.
84. (10.5)	System must utilize the MI-Login (Single Signon) portal to log into the system.	Y					OnBase supports single sign-on integration with several leading technologies including Active Directory (AD), Azure AD, and Active Directory Federation Services (ADFS). Many other proprietary authentication methods are also supported. Integration with Azure Active Directory or SAML is commonly used today.

Documentation and Standards							
85. (11.7)	Application/System documentation must provide FAQ and/or Support Information for frequent issues staff/users may encounter	Y					In addition to the user guides provided with training, help documentation is available within the OnBase Clients. Module Reference Guides (MRG) are also available for Admins. MRG's include information on installation, configuration, usage, and troubleshooting.
Product Development							
86. (12.1)	The application must follow the SUITE testing processes and documentation of testing and testing types/levels must be provided	Y					i3-ImageSoft will work with MSDHA to adhere to the guidelines in SUITE testing process. Hyland OnBase goes through rigorous testing prior to production release to the Hyland customer base. i3-ImageSoft will work with MSHDA to test specific configurations/setup of the MSHDA specific OnBase solution.
Application Security							
87. (13.3)	A solution must comply with any of the following application and data processing standards: SOC II Type 2 or higher Certification	Y					i3-ImageSoft hosted environment will comply with this requirement
88. (13.5)	MSHDA must have the ability to assess the data with retention schedules negotiated by MSDHA	Y					Records Management allows for retention schedules to be created based on MSHDA defined criteria.
89. (13.6)	System must have ability to purge records based on retention schedule	Y					Records can be automatically purged based on retention schedules or sent for review/approval before purging of records.
Identity Management							
90. (14.1)	The application must provide user authentication methods, based on risk and severity level to protect sensitive data and restrict access to only those intended	Y					The security model used in the OnBase system provides for the segregation of data between users, as well as the ability to limit the product functionality available for each user. User Groups and Rights provides for the assignment or restriction of basic and advanced OnBase features. Privileges can be

							assigned in an extremely granular manner in OnBase. This includes securing applications, document types, folders, and features like the ability to edit. Users can also be given read only rights to specific keyword types, or the keyword values themselves can be hidden. Indexing Limits can also be assigned to a user group, in order to limit a user's ability to index documents with specific keyword values.
91. (14.2)	First-time passwords must be set to a unique value for each user and each user change this initial password immediately upon first use	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
92. (14.3)	Access rights for any terminated user must be immediately revoked	Y					User accounts can be locked or removed as needed.
93. (14.4)	Group, shared, or generic accounts and passwords are prohibited	Y					Each user must have their own password.
94. (14.5)	User passwords must be changed at least every 60 days	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
95. (14.6)	All passwords must have a minimum password length of at least fifteen (15) characters	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
96. (14.7)	All passwords must contain characters from three of the following four categories: [a] Uppercase alphabet characters (A–Z). [b] Lowercase alphabet characters (a–z). [c] Arabic numerals (0–9). [d] Non alphanumeric characters (for example, !\$,%)	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
97. (14.8)	A new individual password for a specific user account must be different from any of the last 24 passwords for that user account	Y					Password policies can be created within OnBase, but most customers use another authentication provider like

							Active Directory which will handle password management outside of OnBase.
98. (14.9)	Repeated access attempts must be limited by locking out the user after six (3) consecutive unsuccessful attempts	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
99. (14.1)	System must enforce a limit of three invalid logon attempts within a fifteen minute time period during a user session upon which the account/node is automatically locked for a minimum period of 30 minutes or until released by an administrator	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
100. (14.11)	A user must re-enter his or her password to re-activate the session after more than 15 minutes of idle time	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
101. (14.12)	A password cannot at any time be the same as a user ID	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
102. (14.13)	A user's identity must be verified before performing a password reset.	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
103. (14.14)	Enforce at least one character change when creating new passwords.	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
104. (14.15)	First-time passwords must be set to a unique value for each user and each user change this initial password immediately upon first use	Y					Password policies can be created within OnBase, but most customers use another authentication provider like

							Active Directory which will handle password management outside of OnBase.
105. (14.16)	Allows the use of a temporary password for system logons only with an immediate change to a permanent password.	Y					Password policies can be created within OnBase, but most customers use another authentication provider like Active Directory which will handle password management outside of OnBase.
1068. (14.17)	Access rights for any terminated user must be immediately revoked	Y					User accounts can be locked or removed as needed.
107. (14.18)	Any Service accounts must contain at least 25 characters from the following :[a] Uppercase alphabet characters (A–Z). [b] Lowercase alphabet characters (a–z). [c] Arabic numerals (0–9). [d] Non alphanumeric characters (for example, !\$#,%) and must be randomly generated or the use of Active Directory Managed Services Accounts when possible		Y				Service Accounts are configurable and can follow this criterion if needed.
108. (14.19)	Group, shared, or generic accounts and passwords are prohibited	Y					Each user must have their own password.
109. (14.2)	System must have a pop up that appears every time a user logs in which cannot be bypassed. MSHDA will provide verbiage to be displayed that each user has to agree to.	Y					A login screen is presented to users when authenticating.
110. (14.21)	Restrict the processing of personally identifiable information to only that which is compatible with the identified purpose(s). (Role based)	Y					Personally Identifiable Information (PII) data can be protected with user security, security keywords, and encryption.
System Administration and Licensing							
111. (16.2)	Application/System documentation must provide access to FAQ and/or Support Information for frequent issues administrative staff may encounter	Y					In addition to the user guides provided with training, help documentation is available within the OnBase Clients. Module Reference Guides (MRG) are also available for Admins. MRG's include information on installation, configuration, usage, and troubleshooting.
112. (16.3)	Documentation must provide the anticipated frequency and requirements of patch, break-fix, minor, and major releases	Y					OnBase will typically release one major and one minor release each year with subsequent patches as needed.

							Documentation and Release notes for these will be made available to customers.
Application Design							
113. (17.3)	Mobile compatible	Y					OnBase includes multiple client options including a browser-based Web Client, a ribbon bar Windows Style Client, and a Mobile Client. OnBase also includes a Web App Builder to create client interfaces based on specific user types or roles. This allows for a browser-based experience that is more streamlined and simplified.
Document Management							
114. (3.12)	The system must allow individual files to be bundled together where all documents that were linked can be viewed together in a specific order.	Y					OnBase supports dynamic, content sensitive, document linking capabilities via cross-referencing. OnBase cross-referencing provides the ability to link documents based on like values. Documents can be linked across a single application or different applications, as long as there is a common index value. Static cross-referencing is also available by “stapling” documents together via a drag-and-drop, or accumulating documents into an envelope.
Technical							
Application Security							
115. (13.7)	The system must allow administrator to set maximum size limits on attachments added by user.	Y					Admins can set upload size limits.

SCHEDULE B - PRICING

Table 1: Cost Summary

Item	Cost \$
Software (With Discount)	\$1,694,493.13
Maintenance & Support	\$187,042.63
Hosting	\$414,422.35
Implementation	\$363,200.00
Total	\$2,659,158.11

Table 2: Detailed Cost Breakdown

	Product	Annual Unit Cost	Units	Year 1	Year 2	Year 3	Year 4	Year 5	TOTAL
OnBase Software (Annual Subscription)									
Standard Service Level (On-Premise) Tier 1 (1-25)	ONB-SUB-PW	\$1,200.00	25	\$30,000.00	\$31,500.00	\$33,075.00	\$34,728.75	\$36,465.19	\$165,768.94
Standard Service Level (On-Premise) Tier 2 (26-50)	ONB-SUB-PW	\$1,100.00	25	\$27,500.00	\$28,875.00	\$30,318.75	\$31,834.69	\$33,426.42	\$151,954.86
Standard Service Level (On-Premise) Tier 3 (51-100)	ONB-SUB-PW	\$1,000.00	50	\$50,000.00	\$52,500.00	\$55,125.00	\$57,881.25	\$60,775.31	\$276,281.56
Standard Service Level (On-Premise) Tier 4 (101-200)	ONB-SUB-PW	\$900.00	100	\$90,000.00	\$94,500.00	\$99,225.00	\$104,186.25	\$109,395.56	\$497,306.81
Standard Service Level (On-Premise) Tier 5 (201-500)	ONB-SUB-PW	\$800.00	120	\$96,000.00	\$100,800.00	\$105,840.00	\$111,132.00	\$116,688.60	\$530,460.60
Document Composition & Packaging	ONB-SUB-DCP	\$20,000.00	1	\$20,000.00	\$21,000.00	\$22,050.00	\$23,152.50	\$24,310.13	\$110,512.63
Hyland Discount (if signed by 5/31/2024)				(\$31,350.00)	(\$32,918.55)	(\$34,564.43)	(\$37,156.70)	(\$39,943.38)	(\$175,933.06)
OnBase Subtotal				\$282,150.00	\$296,256.45	\$311,069.32	\$325,758.74	\$341,117.83	\$1,556,352.34
i3-ImageSoft Software (Annual Subscription)									
TrueSign User Tier 1 - Enterprise	IS-TSIGN-USER_Enterprise	\$25,000.00	1	\$25,000.00	\$26,250.00	\$27,562.50	\$28,940.63	\$30,387.66	\$138,140.79
i3-ImageSoft Customer Care	IS-CUSTOMERCARE	\$33,850.00	1	\$33,850.00	\$35,542.50	\$37,319.63	\$39,185.61	\$41,144.89	\$187,042.63
i3-ImageSoft Government Azure Hosting Annual Fee (2TB annually, No Backfile)		\$75,000.00	1	\$75,000.00	\$78,750.00	\$82,687.50	\$86,821.88	\$91,162.97	\$414,422.35
i3-ImageSoft Subtotal				\$133,850.00	\$140,542.50	\$147,569.63	\$154,948.12	\$162,695.52	\$739,605.77
Implementation				363,200.00					363,200.00
TOTAL				\$779,200.00*	\$436,798.95	\$458,638.95	\$480,706.86	\$503,813.35	\$2,659,158.11

*See Tables 3 & 4 for payment milestones.

Table 3: Year 1 Payment Milestones

Num	Payment	When	Amount
Recurring Software & Hosting			
1	Hyland Subscription Software (100%)	Invoiced when Project Signed	\$282,150.00
2	i3-ImageSoft Software (100%)	Invoiced prior to software implementation or development services performed	\$25,000.00
3	Hosting (100%)	Invoiced prior to software implementation or development services performed	\$75,000.00
Professional Services			
4	Services	Billed monthly according to Milestone Payment table below	\$363,200.00
5	Customer Care	Prorated and due 30 days after Go-Live	\$33,850.00
TOTAL			\$779,200.00

Table 4: Implementation Payment Milestones

Contractor may invoice the State no more frequently than monthly for the following milestones completed and all associated deliverables approved by the State during the prior month.

Phase/Milestone	Deliverable	Payment
Project Planning & Initiation	<p>Deliverable Includes:</p> <ul style="list-style-type: none"> - Planning activities - Initial Project Plan - Project Kickoff <p><i>* Milestone will be completed upon delivery of Project Kickoff Notes and Initial Project Plan</i></p>	\$35,000.00
Business Analysis & Design	<p>Deliverable Includes:</p> <ul style="list-style-type: none"> - Requirements gathering (generally onsite) - Creation of Solution Requirements Document ("SRD") <p><i>* Milestone will be completed upon delivery of SRD</i></p>	\$70,000.00
Build and System Test	<p>Deliverable Includes:</p> <ul style="list-style-type: none"> - Development of solution in three (3) environments - Demonstrations as dictated by Project Plan - i3-ImageSoft internal system testing - Delivery of solution for User Acceptance Testing ("UAT") <p><i>*Milestone will be completed upon delivery of the solution for testing</i></p>	\$105,000.00
End User and System Administrator Training	<p>Deliverable Includes:</p> <ul style="list-style-type: none"> - Documentation and training as defined in the SOW - May include UAT and End User Training - Register Customer resources for Hyland Trainings <p><i>*Milestone will be completed upon Customer receipt of training documentation and training efforts as determined by the SOW</i></p>	\$30,700.00
User Acceptance Testing	<p>Deliverable Includes:</p> <ul style="list-style-type: none"> - Support during UAT - Frequent review meetings - Resolution of project issues and bugs during UAT <p><i>*Milestone will be completed upon Customer signoff of UAT</i></p>	\$35,000.00
Production Cutover (Go Live)	<p>Deliverable Includes:</p> <ul style="list-style-type: none"> - Migration of solution to one (1) environment (or as determined by SOW) - System Administrator Handoff meeting and documentation <p><i>*Milestone will be completed when solution is migrated to Production environment, System Administrator meeting is complete when documentation is delivered</i></p>	\$35,000.00

Post Production Support	Deliverable Includes: - Post Go-Live support duration as defined in the SOW - Resolution of in-scope project issues and bugs - Transition to Customer Care *Milestone will be completed upon transition to Customer Care	\$17,500.00
Project Management	Deliverable Includes: - Maintenance of Project Plan - Regular status reports and meetings - Communication Plan - Issue identification and escalation - Risk management - Active management to maintain scope, schedule, and budget * Milestone will be completed thirty (30) days post Production Go-Live date	\$35,000.00
	TOTAL	\$363,200.00

Pricing Assumptions:

Contractor represents that the following activities will meet the requirements listed in Business Specifications Worksheet. I3-ImageSoft will complete the following activities as part of the Build activities for this implementation:

- Complete Hosting Server/Environment Review
- i3-ImageSoft Hosting One-Time Setup
- OnBase Web Server Installation (external use)
- OnBase and i3-ImageSoft Software Installation
- Setup Security and Microsoft Active Directory Integration
- Setup Security and Federated Service ("ADFS") Integration / SAML
- Configure HIS (Hyland Identity Service)
- OnBase Configuration (disk groups, document types, keywords, notes, cross references, EDM Services (if required), custom queries (if required, up to four (4) queries))
- Configuration of DIP Process (four (4) process with no preprocessing)
- Configure (4) Single File Cabinet and Sub-folders (two (2) levels with subfolder based upon document type)
- Configure Document Retention (maximum of twenty-five (25) document types)
- Configure Advance Capture (up to 6 templates)
- Configure Reporting Dashboards (up to two (2) dashboards)
- Install and Configure Outlook Integration
- Install and Configure Microsoft Office Integration (Word, Excel, and PowerPoint)
- Configure Electronic Unity Forms (up to 10 forms)
- Configure Full-Text (up to ten (10) catalogs)
- Configure Document Composition Templates (up to three (3) templates)
- Configure OnBase Application Enabler with Customer LOB Application (for document and/or folder retrieval/indexing) - Emphasys
- Configure OnBase Application Enabler with Customer LOB Application to Create/Populate eForm (four (4) screens/single form) - Emphasys
- Autofill Integration
- CSV File to Customer Line-of-Business Application
- Configure TrueSign Standard OnBase Integration

The following workflows will be completed:

- Signing Workflow (includes scope for a single document signing workflow, max four (4) queues)
- Eligibility
- Lease-up
- Annual Re-Examination
- Interim Re-Examination
- Hearings

Workflows will be defined and documented as part of the Build/Analysis Phase of the project and the customer will sign off on the Solution Requirements Document to complete the scope of the Build.

I3-ImageSoft will provide the following Training Courses:

Solution Training Classes - Train-the-Trainer Methodology	# of Sessions
Includes both preparation time and training for up to ten (10) people	
OnBase Functional and Scan Training (Unity Client)	2
OnBase Business Automation Training - Workflow	2
Conduct TrueSign Functional Training	2
Conduct System Administrator Solution Knowledge Transfer	2

Solution Certification and Online Training	# of People
Hyland Facilitated Classes	
System Administration (per person)	4
Introduction to Workflow (per person)	4

Optional Future Ancillary Services

The labor rates in the table below will apply to optional future ancillary services.

Staffing Category	Onsite Hourly Rate (\$)	Offsite Hourly Rate (\$)
Professional Services	\$240.00	\$210.00

Optional additional storage will be provided upon State request at the following rate:

Hosting Additional Storage (per TB annually)	\$1,000 per TB, per year
---	--------------------------

Travel and Expenses

The State does not pay for overtime or travel expenses.

SCHEDULE C - INSURANCE REQUIREMENTS

1. General Requirements. Contractor, at its sole expense, must maintain the insurance coverage as specified herein for the duration of the Term. Minimum limits may be satisfied by any combination of primary liability, umbrella or excess liability, and self-insurance coverage. To the extent damages are covered by any required insurance, Contractor waives all rights against the State for such damages. Failure to maintain required insurance does not limit this waiver.

2. Qualification of Insurers. Except for self-insured coverage, all policies must be written by an insurer with an A.M. Best rating of A- VII or higher unless otherwise approved by DTMB Enterprise Risk Management.

3. Primary and Non-Contributory Coverage. All policies for which the State of Michigan is required to be named as an additional insured must be on a primary and non-contributory basis.

4. Claims-Made Coverage. If any required policies provide claims-made coverage, Contractor must:

- a. Maintain coverage and provide evidence of coverage for at least 3 years after the later of the expiration or termination of the Contract or the completion of all its duties under the Contract;
- b. Purchase extended reporting coverage for a minimum of 3 years after completion of work if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract.

5. Proof of Insurance.

- a. Insurance certificates showing evidence of coverage as required herein must be submitted to DTMB-RiskManagement@michigan.gov within 10 days of the contract execution date.
- b. Renewal insurance certificates must be provided on annual basis or as otherwise commensurate with the effective dates of coverage for any insurance required herein.
- c. Insurance certificates must be in the form of a standard ACORD Insurance Certificate unless otherwise approved by DTMB Enterprise Risk Management.
- d. All insurance certificates must clearly identify the Contract Number (e.g., notated under the Description of Operations on an ACORD form).
- e. The State may require additional proofs of insurance or solvency, including but not limited to policy declarations, policy endorsements, policy schedules, self-insured certification/authorization, and balance sheets.
- f. In the event any required coverage is cancelled or not renewed, Contractor must provide written notice to DTMB Enterprise Risk Management no later than 5 business days following such cancellation or nonrenewal.

6. Subcontractors. Contractor is responsible for ensuring its subcontractors carry and maintain insurance coverage.

7. Limits of Coverage & Specific Endorsements.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Personal & Advertising Injury \$2,000,000 Products/Completed Operations \$2,000,000 General Aggregate	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
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.	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

8. Non-Waiver. This Schedule C is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract, including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State.

SCHEDULE D – SERVICE LEVEL AGREEMENT (CONTRACTOR HOSTED)

IF THE SOFTWARE IS CONTRACTOR HOSTED, then the following applies:

1. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract Terms and Conditions. **“Actual Uptime”** means the total minutes in the Service Period that the Solution is Available.

“Available” and **“Availability”** have correlative meanings and mean the Hosted Services and Software are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract without material performance degradation or inoperability of the Hosting Services or Software, in whole or in part.

“Availability Requirements” means the percentage of time in a Service Period, as set forth in this Schedule, that the Hosted Services and/or Software must be Available, excluding time the Hosted Services and/or Software is not Available solely because of one or more Exceptions.

“Availability Service Level Credits” means a credit of Fees, which credit is payable to the State for failure to meet the Availability Requirement, as set forth in this Schedule.

“Contact List” means a current list of Contractor contacts and telephone numbers set forth in the attached **Schedule D – Attachment 1** to this Schedule to enable the State to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.

“Corrective Action Plan” means Contractor's written analysis of root causes of Service Errors and/or a Delinquency and Contractor's plan for correction of same, as required by and in such detail as required by and in such detail as required by this Schedule, and which upon written approval by the State, will constitute a Change Notice.

“Critical Service Error” has the meaning set forth in **Subsection 3.6, Solution Support Service Level Table**.

“Exceptions” means Scheduled Downtime or a degradation or inoperability of the Hosted Services solely because of failure of the State's or its Authorized Users' internet connectivity.

“High Service Error” has the meaning set forth in **Subsection 3.6, Solution Support Service Level Table**.

“Low Service Error” has the meaning set forth in **Subsection 3.6, Solution Support Service Level Table**.

“Medium Service Error” has the meaning set forth in **Subsection 3.6, Solution Support Service Level Table**.

“Resolve”, “Resolved”, “Resolution” and correlative capitalized terms mean, with respect to any particular Support Request, that Contractor has corrected the Service Error that prompted that Support Request and that the State has confirmed such correction and its acceptance of it in writing.

“RPO” or **“Recovery Point Objective”** means the maximum amount of potential data loss in the event of a disaster.

“RTO” or **“Recovery Time Objective”** means the maximum period of time to fully restore the Hosted Services in the case of a disaster.

“**Scheduled Downtime**” means a scheduled outage of the Hosting Services or Software, or a scheduled period of time during which Contractor is not required to meet the Availability Requirements, as set forth in this Schedule.

“**Scheduled Uptime**” means the total minutes in the Service Period.

“**Service Availability Report**” means a report that describes the Availability and other performance of the Hosted Services and Software during the calendar month as compared to the Availability Requirement.

“**Service Error**” means any failure of any Hosted Service or the Software to be Available or otherwise perform in accordance with the Contract.

“**Service Availability Failure**” means the Availability Requirements are not met in a Service Period.

“**Service Level Metrics**” means the required Support Request Response and Resolution times referred to in the Solution Support Service Level Table.

“**Service Period**” means each calendar month during the Term and any additional period during which Contractor does or is required to provide the Solution.

“**Solution Support Services**” means the maintenance and support services Contractor must provide as part of any Solution Contractor provides, as set forth in this Schedule.

“**Support Hours**” means 8am to 5pm Eastern, Monday through Friday.

“**Support Service Level Credits**” means the credit set forth in the Solution Support Service Level Credit Table.

“**Support Service Level Failure**” means a failure to meet the Service Level Metrics set forth in the Solution Support Service Level Table.

“**Support Request**” means the State’s request for Contractor to Respond to and Resolve a Service Error.

“**Support Request Classification**” means the type and/or severity designation of a Support Request according to and corresponding to the Service Error Classification of a Service Error that is the subject of a Support Request.

“**Support Request Response Time**” means the period of time beginning when Contractor receives a Support Request, within which Contractor must acknowledge, in writing, its receipt of the Support Request, as set forth in the Service Level Table.

2. Service Availability and Available Service Level Credits.

2.1 Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each “**Service Period**”, at least 99.8% of the time. The Availability Requirement will be calculated for the Service Period as follows: $(\text{Actual Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \div (\text{Scheduled Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \times 100 = \text{Availability}$.

2.2 Exceptions. No period of Hosted Services and/or Software degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to one or more **Exceptions**.

2.3 Scheduled Downtime. Contractor must notify the State at 24 hours in advance of all **Scheduled Downtime**. Scheduled Downtime will: (a) last no longer than 5 hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week;

provided that Contractor may request the State to approve extensions of Scheduled Downtime above 5 hours, and such approval by the State may not be unreasonably withheld or delayed.

2.4 Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than no more than 3.5 seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

2.5 Service Availability Reports. Within 30 days after the end of each Service Period, Contractor will provide to the State Service Availability Report. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services and Software relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

2.6 Remedies for Service Availability Failures.

(a) In the event of a Service Availability Failure, Contractor will issue to the State the Availability Service Level Credits described in the Service Availability Table below calculated as a percentage of the Fees payable for Hosted Services and Software provided during the applicable Service Period:

SERVICE AVAILABILITY TABLE

Availability	Availability Service Level Credits
≥99.8%	None
<99.8% but ≥98.0%	10%
<98.0% but ≥95.0%	20%
<95.0% but ≥90.0%	40%
<95.0%	100%

(b) Any Availability Service Level Credits due under this **Subsection** will be applied in accordance with payment terms of the Contract.

(c) If a Service Availability Failure occurs in any 2 of 4 consecutive Service Periods, then, in addition to all other remedies available to the State, the State, in its sole discretion, consider it to be a material breach of the Contract.

3. Solution Support and Maintenance Services. Contractor will provide Solution maintenance and support services in accordance with the provisions of this **Section 3**. The Solution Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges, other than as stated in **Schedule B – Pricing Schedule**.

3.1 Support Service Responsibilities. Contractor will:

- (a) resolve all Service Errors in accordance with the **Solution Support Service Level Table**, including by providing defect repair, programming corrections and remedial programming;
- (b) provide unlimited telephone support during Support Hours.
- (c) provide unlimited online support during Support Hours,
- (d) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and
- (e) respond to and Resolve Support Requests as specified in this **Section 3**.

3.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

- (a) proactively monitoring on a 24 hour by 7 day basis all Hosted Service and Software functions, servers, firewall and other components of Hosted Service and Software security;

(b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service and Software, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Contractor receives knowledge that the Hosted Service, Software or any of its function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein):

(i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii) If Contractor's facility check in accordance with clause (i) above confirms a Hosted Service or Software outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Subsections 3.6**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) Notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

3.3 Service Maintenance. Contractor will continuously maintain the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

(a) all updates, bug fixes, enhancements, Maintenance Releases, New Versions and other improvements to the Hosted Services and Software, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; provided that Contractor shall consult with the State and is required to receive State approval prior to modifying or upgrading Hosted Services and Software, including Maintenance Releases and New Versions of Software; and

(b) all such services and repairs as are required to maintain the Hosted Services and Software or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosted Services and Software, so that the Hosted Services and Software operate properly in accordance with the Contract and this Schedule.

3.5 Support Requests. The State may submit a Support Request when the State experiences a Service Error. The State will include in its Support Request the applicable Support Request Classification and a description of the Service Error and the time the State first observed the Service Error. The State will submit each Support Request by e-mail or telephone.

3.6 Solution Support Service Level Table. As set out in the **Solution Support Service Level Table** below, applicable Service Level Metrics will be measured from the time Contractor receives a Support Request until the respective times Contractor has (a) responded to that Support Request, in the case of Support Request Response time and (b) Resolved that Support Request, in the case of Support Request Resolution time. Contractor shall respond to and Resolve all Support Requests within the following times based on the State's Support Request Classification, subject to the State's written agreement to revise such designation after Contractor's investigation of the reported Service Error:

RESPONSE AND RESOLUTION TIME SERVICE TABLE

Support Request Classification	Definition	Service Level Metric for Required Support Request Response Time	Service Level Metric for Required Support Request Resolution Time)
Critical Service Error	Any Service Error comprising or causing any of the following events or effects issue affecting the entire system or a single critical production function: (a) Software down or operating in materially degraded state; (b) Data integrity at risk; (c) Material financial impact; (d) Widespread access interruptions; or (e) Classified by the state as a Critical Service Error	Contractor shall acknowledge receipt of a Support Request within 30 minutes.	For Software: Contractor shall Resolve the Support Request as soon as practicable and no later than 4 hours after Contractor's receipt of the Support Request.
High Service Error	(a) A Critical Service Error for which the State has received, within the Resolution time for Critical Service Errors, a work-around that the State has accepted in writing; or (b) Primary component failure that materially impairs Software's performance; (c) Data entry or access is materially impaired on a limited basis; or (d) performance issues of severe nature impacting critical processes	Contractor shall acknowledge receipt of a Support Request or, where applicable, the State's written acceptance of a Critical Service Error work-around, within 24 hours.	Contractor shall Resolve the Support Request as soon as practicable and no later than 2 Business Days after Contractor's receipt of the Support Request or, where applicable, the State's written acceptance of a Critical Service Error work-around.
Medium Service Error	An isolated or minor Error in the Software that meets any of the following requirements: (a) does not significantly affect Software functionality; (b) can or does impair or disable only certain non-essential Software functions; or (c) does not materially affect the State's use of the Software	Contractor shall acknowledge receipt of the Support Request within 2 Business Days.	Contractor shall Resolve the Support Request as soon as practicable and no later than 10 Business Days after Contractor's receipt of the Support Request. If Medium Service Error has not been resolved in 10 Business Days, the State may resubmit as a High Service Error.

Low Service Error	Request for assistance, information, or services that are routine in nature.	Contractor shall acknowledge receipt of the Support Request within 5 Business Days.	Contractor shall Resolve the Support Request as soon as practicable and no later than 60 Business Days after Contractor's receipt of the Support Request. If Low Service Error has not been resolved in 60 Business Days, the State may resubmit as a Medium Service Error.
--------------------------	--	---	--

3.7 Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within 60 minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Project Manager and Contractor's management or engineering personnel, as appropriate.

3.8 Support Service Level Credits. If the Contractor fails to meet a Service Level Metric for Support Request Response and/or Resolution Time, the State will be entitled to the corresponding Support Service Level Credits specified in the table below.

Solution Support Service Level Credit Table:

Support Request Classification	Support Service Level Credits (For Support Service Level Failure regarding Support Request Response Time)	Support Service Level Credits (For Support Service Level Failure regarding Support Request Resolution Time)
Critical Service Error	5% of the Fees for the month in which the initial Service Level Failure begins and 5% of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	5% of the Fees for the month in which the initial Service Level Failure begins and 5% of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
High Service Error	3% of the Fees for the month in which the initial Service Level Failure begins and 3% of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	3% of the Fees for the month in which the initial Service Level Failure begins and 3% of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.

3.9 Corrective Action Plan. If two or more Critical Service Errors occur in any 60 day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within 10 Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

4. Issuance of Applicable Credits. Contractor will, for each invoice period, issue to the State, together with Contractor's invoice for such period, a written acknowledgement setting forth all Availability Service Credits and Support Level Credits to which the State has become entitled during that invoice period. Contractor shall pay the amount of applicable credit(s) as a debt to the State within 15 Business Days of issue of the applicable credit from the amount payable by the State to Contractor pursuant to such invoice. If the Fees for Hosted Services and/or the Support Fee is paid other than monthly, the applicable fee will be converted to its monthly equivalent for purposes of determining the Availability Service Credit and/or Support Service Level Credit based on the percentages in the applicable tables in this Schedule.

5. Additional Remedies for Service Level Failures. Contractor's repeated failure to meet the Service Level Metric(s) for Resolution of any Critical Service Errors or High Service Errors, or any combination of such Errors, within the applicable Resolution time set out in the Solution Support Service Level Table will constitute a material breach of the Contract.

6. Data Storage, Backup, Restoration and Disaster Recovery. Contractor must maintain or cause to be maintained backup redundancy and disaster avoidance and recovery procedures designed to safeguard State Data and the State's other Confidential Information, Contractor's Processing capability and the availability of the Hosted Services and Software, in each case throughout the Term and at all times in connection with its actual or required performance of the Services hereunder. All backed up State Data shall be located in the United States. The force majeure provisions of this Contract do not limit Contractor's obligations under this section.

6.1 Data Storage. Contractor will provide sufficient storage capacity to meet the needs of the State. Contractor will provide 2 terabytes (TB) of storage initially and 2 additional TB each year thereafter at no additional cost. If needed, the State may purchase additional storage at the rate listed in the Pricing Schedule.

6.2 Data Backup. Contractor will conduct, or cause to be conducted, daily back-ups of State Data and perform, or cause to be performed, other periodic offline back-ups of State Data on at least a weekly basis and store and retain such back-ups as specified in **Schedule A**. Contractor must, within 5 Business Days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of State Data in the format specified by the State.

6.3 Data Restoration. If the data restoration is required due to the actions or inactions of the Contractor or its subcontractors, Contractor will promptly notify the State and complete actions required to restore service to normal production operation. If requested, Contractor will restore data from a backup upon written notice from the State. Contractor will restore the data within 1 Business Day of the State's request. Contractor will provide data restorations at its sole cost and expense.

6.4 Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a **Recovery Point Objective (RPO) of 4 hours**, and a **Recovery Time Objective (RTO) of 4 hours** (the "**DR Plan**") and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor's current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule F**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within 15 days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 4**; and provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

First line of support is our Customer Care Team. The Customer Care contact information is below:

- Customer Care Portal: <https://portal.imagesoftinc.com/Login.aspx?ReturnUrl=%2f>
- Customer Care Support Telephone Number: 248-948-8100 Option 2

Escalation contacts, in order, for Support are as follows:

Senior Account Executive: Tim Zarzycki

403 S. Main St., Royal Oak, MI 48067

586-942-8423

tzarzycki@i3verticals.com

VP of Enterprise Support – Steve Michelin

403 S. Main St., Royal Oak, MI 48067

810-444-7462

smichelin@i3verticals.com

SCHEDULE E – DATA SECURITY REQUIREMENTS

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract.

“**Contractor Security Officer**” has the meaning set forth in **Section 2** of this Schedule.

“**FedRAMP**” means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

“**FISMA**” means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014.)).

“**Hosting Provider**” means any Permitted Subcontractor that is providing any or all of the Hosted Services and/or Operating Environment under this Contract.

“**NIST**” means the National Institute of Standards and Technology.

“**PCI**” means the Payment Card Industry.

“**PSP**” or “**PSPs**” means the State’s IT Policies, Standards and Procedures.

“**SSAE**” means Statement on Standards for Attestation Engagements.

“**Security Accreditation Process**” has the meaning set forth in **Section 6** of this Schedule

2. Security Officer. Contractor will appoint a Contractor employee to respond to the State’s inquiries regarding the security of the Solution who has sufficient knowledge of the security of the Solution and the authority to act on behalf of Contractor in matters pertaining thereto (“**Contractor Security Officer**”).

3. Contractor Responsibilities. Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to:

- (a) ensure the security and confidentiality of the State Data;
- (b) protect against any anticipated threats or hazards to the security or integrity of the State Data;
- (c) protect against unauthorized disclosure, access to, or use of the State Data;
- (d) ensure the proper disposal of any State Data in Contractor’s or its subcontractor’s possession; and
- (e) ensure that all Contractor Personnel comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor’s data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at <https://www.michigan.gov/dtmb/policies/it-policies>.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the Solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

4. Acceptable Use Standard. To the extent that Contractor has access to the State’s IT environment, Contractor must comply with the State’s Acceptable Use Standard, see <https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/IT-Policy/13400013002-Acceptable-Use-of-Information-Technology-Standard.pdf>. All Contractor Personnel will be required, in writing, to agree to the State’s Acceptable Use Standard before accessing State systems or Data. The State reserves the right to terminate Contractor’s and/or subcontractor(s) or any Contractor Personnel’s access to State Systems if the State determines a violation has occurred.

5. Protection of State's Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause;

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

5.3 ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, backed up in the United States, its territories or Canada;

5.4 ensure that any Customization development work is performed in the United States;

5.5 ensure the data center(s) in which Software and State Data resides minimally meets Uptime Institute Tier 3 standards (<https://www.uptimeinstitute.com/>), or its equivalent;

5.6 maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State Data that complies with the requirements of the State's data security policies as set forth in this Contract, and must, at a minimum, remain compliant with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

5.7 Throughout the Term, Contractor must not provide any part of the Solution from the list of excluded parties in the [System for Award Management \(SAM\)](#) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services.

5.8 provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data, consistent with best industry practice and applicable standards (including, but not limited to, compliance with FISMA, NIST, CMS, IRS, FBI, SSA, HIPAA, FERPA and PCI requirements as applicable);

5.9 take all reasonable measures to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Solution against "malicious actors" and others who may seek, without authorization, to destroy, disrupt, damage, encrypt, modify, copy, access or otherwise use Hosted Services or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Solution; (ii) State Data from being commingled with or contaminated by the data of other customers or their users of the Solution; and (iii) unauthorized access to any of the State Data;

5.10 ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.11 ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML), Open Authentication (OAuth) or comparable State approved mechanisms;

5.12 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

5.13 Contractor must permanently sanitize or destroy the State's information, including State Data, from all media both digital and nondigital including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. Contractor must sanitize information system media, both digital and non-digital, prior to disposal, release out of its control, or release for reuse as specified above.

6. Security Accreditation Process. Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State's automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor's security controls within two weeks of the State's request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system's controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to create or assist with the creation of State approved POAMs, perform related remediation activities, and provide evidence of compliance. The State will make any decisions on acceptable risk, Contractor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk. Failure to comply with this section will be deemed a material breach of the Contract.

7. Unauthorized Access. Contractor may not access, and must not permit any access to, State Systems, in whole or in part, whether through the Hosted Services or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State Systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this Section. All State-authorized connectivity or attempted connectivity to State Systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

8. Security Audits.

8.1 During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.

8.2 Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract. The State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. If the State chooses to perform an on-site audit, Contractor will, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least 5 Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Hosted Services and their housing facilities and operating environments.

8.3 During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's (if applicable) FedRAMP System Security Plan(s) or SOC 2 Type 2 report(s) to the State within two weeks of the State's request. The System Security Plan and SSAE audit reports will be recognized as Contractor's Confidential Information.

8.4 With respect to State Data, Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

8.5 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8**.

9. Application Scanning. During the Term, Contractor must, at its sole cost and expense, scan all Contractor provided applications, and must analyze, remediate and validate all vulnerabilities identified by the scans as required by the State Web Application Security Standard and other applicable PSPs.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Authenticated interactive scanning of application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST)).

(a) Contractor must either a) grant the State the right to dynamically scan a deployed version of the Software; or b) in lieu of the State performing the scan, Contractor must dynamically scan a deployed version of the Software using a State approved application scanning tool, and provide the State with a vulnerabilities assessment after Contractor has completed such scan. These scans and assessments i) must be completed and provided to the State quarterly (dates to be provided by the State) and for each major release; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

(a) For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code, and for all source code for each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans.

9.3 Software Composition Analysis (SCA) – Third-Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation.

(a) For Software that includes third-party and open source software, all included third-party and open source software must be documented and the source supplier must be monitored by the Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. These scans must be completed for all third-party and open source software initially, for all updated third-party and open source software, and for all third party and open source software in each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans if not provided as part of SAST and/or DAST reporting.

9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

(a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programming interface (API).

(b) Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

10. Infrastructure Scanning.

10.1 Contractor must ensure their infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly and provide the scan's assessments to the State in a format that is specified by the State and used to track the remediation. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements documented in the State's PSPs.

11. Nonexclusive Remedy for Security Breach.

11.1 Any failure of the Solution to meet the applicable requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

SCHEDULE F – DISASTER RECOVERY PLAN

Contractor has presented to the State a Disaster Recovery Plan summary, which is incorporated herein by reference, but is not restated here for security purposes.

SCHEDULE G – TRANSITION IN AND OUT

TRANSITION IN PLAN

Pre-Installation: Initiation and Discovery

i3 Responsibilities:

- Perform solution discovery and design for initial environment build
- Work with i3 PM to create hosting tasks for overall Project Plan
- Set expectations with customer including overall project, solution discovery finalization, training plans, etc.
- Prepare solution data
- Send custom code to via tech support issue to review
- Confirm Installation Resource Assignment and Release ETAs
- Provide data transfer details and credentials for DB and solution files/data upload
- Review and approve custom code (if needed)

Installation

i3 Responsibilities:

- Provide updates to the customer, if needed
- Utilize customer data (if provided)
- Build a “configuration ready” solution as requested
- Create solution release documentation
 - Email announcing release of solution to customer
 - Solution documentation containing key solution information
 - Securely send account credentials to be used with the solution

Post Installation: Implementation, UAT, and Go Live

i3 Responsibilities:

- Provide customer with Release Document
- Provide customer with account credentials
- Review solution (smoke test) for quality/defects within 48 business hours of receipt
- Configure Solution
 - IdP/Single Sign-On
 - Perform final solution configuration (integrations, custom components, etc.)
- Solution Testing
- Schedule Go Live
- Train customer team
- Installation team resource will support solution for 48 (business) hours from release
- Issues discovered after 48 hours must be submitted via Technical Support Issue
- Provide Go Live Support
 - Confirm Go Live date
 - Installations Team will provide a resource for related Go Live activities

TRANSITION OUT PLAN

For Transitioning Customers out of our hosted environment we typically will follow the below key areas to complete a transition plan:

- Written agreement on intent to leave the OnBase system
- Evaluation of existing solution size (number of documents, size of metadata db)
- Determination of preferred transition out delivery method. Does Customer want all data on a physical device, or is a hosted storage location preferred
- Determination of delivery format.

- For eg. Does the Customer want all metadata in a database format, or do they prefer flat file index info
- Determination of cost of exporting of data
- Agreement on payment terms for data export assistance.
- Running of export process
- Delivery of files
- Date Cut off timing of delivered files
- Transition complete.

SCHEDULE H – FEDERAL PROVISIONS ADDENDUM

This addendum applies to purchases that will be paid for in whole or in part with funds obtained from the federal government. The provisions below are required, and the language is not negotiable. Contractor agrees to comply with all obligations under federal rules or regulations for such funding, including but not limited to the provisions contained in this addendum. If any provision below conflicts with the State's terms and conditions, including any attachments, schedules, or exhibits to this Contract, the provisions below take priority to the extent a provision is required by federal law; otherwise, the order of precedence set forth in the Contract applies. Further, Contractor agrees to, through a Contract Change Notice, append or modify specific federal provisions to this Contract, if reasonably necessary to keep the State and Contractor in compliance with federal funding requirements, and comply with the terms set forth therein. Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

A. Equal Employment Opportunity

This Contract is not a “**federally assisted construction contract**” as defined in [41 CFR Part 60-1.3](#).

B. Davis-Bacon Act (Prevailing Wage)

This Contract is not a “**federally assisted construction contract**” as defined in [41 CFR Part 60-1.3](#), nor is it a prime construction contract in excess of \$2,000.

C. Copeland “Anti-Kickback” Act

This Contract is not a “**federally assisted construction contract**” as defined in [41 CFR Part 60-1.3](#).

D. Contract Work Hours and Safety Standards Act

The Contract does not involve the employment of mechanics or laborers.

E. Rights to Inventions Made Under a Contract or Agreement

If this Contract is funded by a federal “funding agreement” as defined under [37 CFR §401.2 \(a\)](#) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” the recipient or subrecipient must comply with [37 CFR Part 401](#), “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency.

F. Clean Air Act and the Federal Water Pollution Control Act

If this Contract is **in excess of \$150,000**, the Contractor must comply with all applicable standards, orders, and regulations issued under the Clean Air Act ([42 USC 7401-7671q](#)) and the Federal Water Pollution Control Act ([33 USC 1251-1387](#)), and during performance of this Contract the Contractor agrees as follows:

(1) Clean Air Act

- (i) The Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
- (ii) The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.
- (iii) The Contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA or the applicable federal awarding agency.

(2) Federal Water Pollution Control Act

- (i) The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
- (ii) The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.

- (iii) The Contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA or the applicable federal awarding agency.

G. Debarment and Suspension

A “contract award” (see [2 CFR 180.220](#)) must not be made to parties listed on the government-wide exclusions in the [System for Award Management](#) (SAM), in accordance with the OMB guidelines at [2 CFR 180](#) that implement [Executive Orders 12549 \(51 FR 6370; February 21, 1986\)](#) and 12689 ([54 FR 34131; August 18, 1989](#)), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than [Executive Order 12549](#).

- (1) This Contract is a covered transaction for purposes of 2 C.F.R. Part 180 and 2 C.F.R. Part 3000. As such, the Contractor is required to verify that none of the Contractor’s principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).
- (2) The Contractor must comply with 2 C.F.R. Part 180, subpart C and 2 C.F.R. Part 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.
- (3) This certification is a material representation of fact relied upon by the State. If it is later determined that the contractor did not comply with 2 C.F.R. Part. 180, subpart C and 2 C.F.R. Part. 3000, subpart C, in addition to remedies available to the State, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.
- (4) The bidder or proposer agrees to comply with the requirements of 2 C.F.R. Part 180, subpart C and 2 C.F.R. Part 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

H. Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (as amended)

Contractor has applied or bid for an award of **more than \$100,000** and shall file the required certification in *Exhibit 1 – Byrd Anti-Lobbying Certification* attached to the end of this Addendum. Each tier certifies to the tier above that it will not and has not used federally appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-federal funds that takes place in connection with obtaining any federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the federal awarding agency.

I. Procurement of Recovered Materials

If this Contract is a procurement to purchase products or items designated by the EPA under [40 C.F.R. part 247](#) during the course of a fiscal year, then under [2 CFR 200.323](#), Contractors must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act.

- (1) In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired:
 - (i) Competitively within a timeframe providing for compliance with the contract performance schedule;
 - (ii) Meeting contract performance requirements; or
 - (iii) At a reasonable price.
- (2) Information about this requirement, along with the list of EPA- designated items, is available at EPA’s Comprehensive Procurement Guidelines web site, <https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program>.
- (3) The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

J. Prohibition on Contracting for Covered Telecommunications Equipment or Services

Contractor acknowledges and agrees that [Section 889\(b\) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 \(the "McCain Act"\)](#), and [2 C.F.R. §200.216](#), prohibit the obligation or expending of federal award funds on certain telecommunication products or with certain entities for national security reasons on or after August 13, 2020.

During performance of this Contract, the Contractor agrees as follows:

(a) *Definitions.* As used in this Section J. Prohibition on Contracting for Covered Telecommunications Equipment or Services ("Section J"):

- (1) the terms "backhaul," "critical technology," "interconnection arrangements," "reasonable inquiry," "roaming," and "substantial or essential component" have the meanings defined in 48 CFR § 4.2101;
- (2) the term "covered foreign country" has the meanings defined in § 889(f)(2) of the McCain Act; and
- (3) the term "covered telecommunications equipment or services" has the meaning defined in § 889(f)(3) of the McCain Act.

(b) *Prohibitions.*

- (1) Unless an exception in paragraph (c) of this Section J applies, neither the Contractor nor any of its subcontractors may use funds received under this Contract to:
 - (i) Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
 - (ii) Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
 - (iii) Enter into, extend, or renew a contract with an entity that uses any covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or
 - (iv) Provide, as part of its performance of this contract, subcontract, or other contractual instrument, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(c) *Exceptions.*

- (1) This Section J does not prohibit Contractor from providing—
 - (i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
 - (ii) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

- (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this Section J to the recipient or subrecipient, unless elsewhere in this contract are established procedures for reporting the information.
- (2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this Section J:
 - (i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer

part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

- (ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this Section J: Any further available information about mitigation actions undertaken or recommended. In addition, the contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

- (e) *Subcontracts*. The Contractor shall insert the substance of this Section J, including this paragraph (e), in all subcontracts and other contractual instruments.

K. Domestic Preferences for Procurements

As appropriate, and to the extent consistent with law, the Contractor should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States. This includes, but is not limited to iron, aluminum, steel, cement, and other manufactured products.

For purposes of this Section K – **Domestic Preferences for Procurements**:

“Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

“Manufactured products” mean items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

L. Affirmative Socioeconomic Steps

For all contracts utilizing federal funding sources subject to Title 2 of the Code of Federal Regulations (C.F.R.) Part 200 issued on or after November 12, 2020, if subcontracts are to be let, the prime contractor is required to take all necessary steps identified in 2 C.F.R. § 200.321(b)(1)-(5) to ensure that small and minority businesses, women’s business enterprises, and labor surplus area firms are used when possible.

M. Copyright and Data Rights

Pursuant to 2 CFR § 200.315(b), the State may copyright any work which is subject to copyright and was developed, or for which ownership was acquired, under a Federal award. The Federal awarding agency reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for Federal purposes, and to authorize others to do so.

N. Additional FEMA Contract Provisions

This Contract does not involve purchases that will be paid for in whole or in part with funds obtained from the Federal Emergency Management Agency (FEMA).

O. Other Federal Contract Provisions

No additional federal provisions currently apply to this Contract.

SCHEDULE H - EXHIBIT 1 – BYRD ANTI-LOBBYING CERTIFICATION

Contractor must complete this certification if the purchase will be paid for in whole or in part with funds obtained from the federal government and the purchase is greater than \$100,000.

APPENDIX A, 44 C.F.R. PART 18 – CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, Title 31, U.S. C. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

The Contractor, i3-ImageSoft, LLC, certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. Chap. 38, Administrative Remedies for False Claims and Statements, apply to this certification and disclosure, if any.

Signature of Contractor's Authorized Official

/s/ _____
Crystal Bell, President of Enterprise Solutions

Date: _____