STATE OF MICHIGAN PROCUREMENT

Department Technology, Management and Budget
Central Procurement Services
320 S Walnut Street Lansing, MI 48933
P.O. Box 30026, Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **260000000965**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	Armedia, LLC	
	8221 Old Courthouse Rd, Suite 300	
	Vienna Virginia 22182	
	James Bailey	
	213-925-2584	
	James.bailey@armedia.com	
	VS0228346	

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

CONTRACT SUMMARY			
DESCRIPTION: Enterprise FOIA System			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
8/1/2026	7/31/2031	5 - 1 Year	7/31/2031
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
N/A		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card ☐ Payment Request (PRC) ☐ Other			☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
N/A			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$6,690,218.84**

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Brice Sample	517-335-9450	sampleb@michigan.gov
DTMB	Jibu John	517-242-4260	JohnJ@michigan.gov

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name and Title

DTMB Central Procurement Services

Agency

Date

SOFTWARE CONTRACT TERMS AND CONDITIONS

These 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 Armedia, LLC ("**Contractor**"), a Georgia limited liability company. This Contract is effective on August 1, 2026 ("**Effective Date**"), and unless terminated, will expire on July 31, 2031 (the "**Term**").

This Contract may be renewed for up to five additional one-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.

"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.

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

"**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.

"Digital Deliverables" means Deliverables, information, and/or content created, provided, or made available by Contractor under this Contract in a digital format, including but not limited to, websites, applications, software, mobile applications, text, images, sounds, videos, controls, animations, links, and documents (including files in the following formats: PDF, word processing, presentation, and spreadsheet).

"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.**

"Hardware" means all computer hardware or other equipment provided by Contractor under this Contract, if any, including but not limited to any related accessories.

"**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 Solution 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, 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.

"Offshore Resources" mean resources, including Contractor Personnel, outside of the United States or its territories.

"**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).

"**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.

"System" has the meaning set forth in **Schedule I**.

"System Acceptance" has the meaning set forth in **Schedule I**.

"System Integration Testing" has the meaning set forth in **Schedule I**.

"**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, queries, prompts, 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 user, device, system or network by or on behalf of the State, including but not limited to any and all works, inventions, data, analyses, information that identifies State or State's intended users' devices or equipment, location information, or other information and materials resulting from any use of the Software by or on behalf of the State's intended users under this Contract, even if not input by a user. User Data does not include any data in the possession of or collected by Contractor prior to or independently of the performance of the Services or prior to any use of the Software under this Contract.

"**Warranty Period**" means the 90 calendar-day period commencing on the date of the State's Acceptance of the Software or System (if Contractor is providing Hardware under this Contract) for which Support Services are provided free of charge.

"**Work Product**" means everything made or created by Contractor, regardless of whether created, developed, or generated by a human, non-human, or some combination thereof, specifically and solely for the State and which is not generally available to Contactor'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. 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 Contract 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 Contract Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Contract 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 Contract 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 Contract Changes; and

(iv) any increase or decrease in Fees resulting from the proposed Contract Changes, which increase, or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Contract 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 Contract 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 Contract 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 Contract Change to those necessary to perform the Contract 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 Contract 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.

(e) The use of Offshore Resources is not permitted under this Contract.

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 will 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 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: (a) when verified by written receipt if sent by courier; (b) when received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Jarrod Barron 320 S. Walnut Lansing, MI 48933 BarronJ1@michigan.gov 517-249-0406	James Bailey 8221 Old Courthouse Rd, Suite 300 Vienna, VA 22182 James.bailey@armedia.com 213-925-2584

4. Insurance. Contractor must maintain the minimum insurances 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, 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.

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 created, developed, or generated exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(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 does 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 all Intellectual Property Rights; and

(ii) irrevocably waives 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 provide 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 deliver and install 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 and installation of the Software. If the State is responsible for Site preparation, 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.

(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)**. Acceptance of the Software may be conditioned upon System Acceptance, if Contractor is providing Hardware, under the terms of this Contract.

10. Non-Software Acceptance.

10.1 If Contractor is providing Hardware under this Contract, Contractor will comply with the requirements for delivery, acceptance and warranty of Hardware as set forth in **Schedule H**.

10.2 System Acceptance. If Contractor is providing Hardware under this Contract, Contractor will comply with the requirements for acceptance testing of the Software and Hardware together as a System, as set forth in **Schedule I**.

10.3 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.**

10.4 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.

10.5 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 plus an additional 10% administrative fee.

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, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other governmental entity if such assignment is made reasonably necessary by operation of controlling law or regulation. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

12. Change of Control. Contractor will notify the State, within 30 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. The State will notify Contractor of any dispute within a reasonable time. 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 at 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 at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

13.6 Taxes. The State is exempt from federal excise tax, state, and local sales taxes, and use taxes if the Solution purchased under this Contract is for the State's exclusive use. Contractor will not include the collection of taxes for which the State is exempt in any invoices or payments related to this Contract. The State is not responsible for taxes imposed or assessed on Contractor.

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 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 90 calendar days, or any longer period agreed to by Contractor, 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.

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. 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 30 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

(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 accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must 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, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

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 30 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 must, for a period of time specified by the State (not to exceed 180 calendar days; the "**Transition Period**"), provide all 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. Such transition assistance may include but is not limited to:

(i) continuing to perform the Services at the established Contract rates;

(ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee;

(iii) taking all 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) Contractor 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 must 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 or other right of any third party;

(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); 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).

17.2 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, 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;

(b) participate in the defense of the proceeding;

(c) employ its own counsel; 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 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,** 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 designs, specifications, or instructions of the State; or

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

19. Disclaimer of Damages and Limitation of Liability.

19.1 Disclaimer of Damages. NEITHER PARTYWILL 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 Limitation of Liability.

(a) 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.

(b) IN NO EVENT WILL THE CONTRACTOR'S AGGREGATE LIABILITY 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 TWO TIMES THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

19.3 Exceptions. Subsections 19.1 (Disclaimer of Damages) and 19.2 (Limitation of Liability) above, will not apply to: (i) Contractor's obligation to indemnify under this Contract; (ii) Contractor's obligations under this Contract regarding Loss or Compromise of State Data; (iii) Contractor's obligations or amounts due under a clause (regardless of how named) providing for liquidated damages; (iv) any loss or claim to the extent the loss or claim is covered by a policy of insurance maintained, or required by this Contract to be maintained, by Contractor; and (v) damages arising from either party's recklessness, bad faith, or intentional misconduct.

20. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 14 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) Work Product

(c) 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

(d) any other data collected, used, Processed, stored, or generated in connection with the Solution, including but not limited to:

(i) personally identifiable information ("**PII**") 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**") 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 or its territories, and not permit any Contractor Personnel to Access any State Data or State Systems from outside of the United States or its territories; 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 or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties.

22.1 Meaning of Confidential Information. For the purposes of this Contract, the term "**Confidential Information**" means all information 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, (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 an 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 an obligation of confidentiality; 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 5 Business Days from the date of termination or expiration, return to the other party 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. 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 State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within 5 Business Days from the date of confirmation 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 calendar 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. Contractor must 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.

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. The State has no obligation to install or use any Maintenance Release or New Versions. 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 Acceptance Tested by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its 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. Artificial Intelligence.

28.1 Model Cards.

(a) Contractor will provide a comprehensive model card for any artificial intelligence (including but not limited to machine learning models, large language models, neural networks, or probabilistic based tools) integrated into the Deliverables. A comprehensive model card will include, at a minimum, model details (name, version, architecture, training methodology); intended uses and known limitations; description of training data and data sources; evaluation metrics and performance benchmarks; fairness, ethical, and safety considerations; and maintenance plan and update history.

(b) Contractor will provide the initial model card prior to deployment of the applicable model and will update the model card promptly upon any material changes to the model. Examples of material changes include but are not limited to retraining of the model, version changes, changes to input data, or known performance deviations such as performance degradation or risk factors that could impact the quality, behavior, or reliability of the Deliverables. Contractor will provide 30-calendar days' advance notice of any material changes to model versions and will conduct regression testing prior to deployment. Material changes to any artificial intelligence models will not degrade performance or increase risk exposure to the State.

(c) Contractor must deliver model cards in a format reasonably acceptable to the State and the model cards must be kept up to date during the Term.

(d) The State reserves the right to audit the accuracy and completeness of any model card and request clarification or supporting evidence for any claims made therein. Contractor will provide the clarification or supporting evidence within 5 Business Days of the State's request. The State may use a qualified independent third-party to conduct and complete or assist in the audit. Contractor will provide reasonable assistance and cooperate with the audit.

28.2 If Contractor integrates a third-party artificial intelligence (including but not limited to machine learning models, large language models, neural networks, probabilistic based tools) into the Deliverables, Contractor will ensure that the third-party artificial intelligence model complies with the auditability and documentation requirements in this Contract.

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 also 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 the Intellectual Property Rights to 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 the license 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 other than Third-Party Components that Contractor has included in its Software Bill of Materials (as described in Schedule A), in an applicable Statement of Work or elsewhere in this Contract, or as otherwise required by this Contract.

(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 license 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 (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;

(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 in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

(l) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.

(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. 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 Work Product Representations and Warranties: Contractor further represents and warrants to the State that:

(a) Contractor has all necessary rights, title, and/or licenses required to create, develop, or generate Work Product and to transfer all ownership rights in Work Product and/or User Data to the State as set forth in Section 7.

(b) Contractor has verified that no third-party intellectual property has been incorporated into any Work Product and/or User Data created, developed, or generated by any nonhuman means used by Contractor.

(c) Contractor is the author and creator of all Work Product.

29.5 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 all 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, sexual orientation, gender identity or expression, 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. 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 a like Solution 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, 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; Termination. 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. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of 5 Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's 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 other than as a result of 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 including transactions with MiDEAL members, and other states (including governmental subdivisions and authorized entities). 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 Digital Deliverables must 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 remediate issues and achieve conformance with the Digital Accessibility Standards in the event of any deficiencies at its sole cost and expense; and

(c) ensure that no changes made by Contractor to any Digital Deliverables will have any adverse effect on conformance to the Digital Accessibility Standards.

45.2 Contractor must, upon the State's written request, provide Digital Deliverables in one or more alternative formats and within timeframes specified by the State.

45.3 State of Michigan Digital Standards Review.

Throughout the Term, Contractor must, upon request from the State, submit documentation or other information regarding accessibility and Contractor's compliance with the Digital Accessibility Standards, including without limitation, a completed accessibility conformance report, such as an Information Technology Industry Council (ITAC) Voluntary Product Accessibility Template (VPAT®), and/or a description of the evaluation methods used to support the Digital Accessibility Standards conformance claims, including, if applicable, any third-party testing.

Prior to Digital Deliverables being accepted, put into production, or as otherwise required by the State, the State may conduct a review to assess accessibility and compliance with the State's Digital Accessibility Standards and Contractor must at its sole cost and expense, remediate all issues resulting from any such review in a manner and timeframe approved in writing by the State.

45.4 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.

45.5 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. However, if this Contract is subject to the Michigan Prevailing Wage Act, MCL 408.1101 et seq. construction mechanics (as defined in MCL 408.1101 (b)) are intended beneficiaries for the limited purposes set forth and as required by MCL 408.1112.

50. Prevailing Wage Act Statutory Provision. As required by MCL 408.1112, if the Michigan Prevailing Wage Act, MCL 408.1101 et seq. applies to this Contract, construction mechanics (as defined in MCL 408.1101 (b)) are intended beneficiaries of the contractual prevailing wage, fringe benefit, and nondiscrimination nonretaliation requirements of the Contract. Any construction mechanic aggrieved by the failure of a Contractor or subcontractor to pay prevailing wages or benefits as specified in this Contract, or by a violation of MCL 408.1107, in addition to any other remedies provided in Public Act 10 of 2023 or by law, may bring an action in a court of competent jurisdiction against the Contractor or subcontractor for damages or injunctive relief and may be awarded reinstatement or other appropriate relief, and all damages sustained, together with actual costs and attorney fees at trial and on appeal. If the Michigan Prevailing Wage Act, MCL 408.1101 et seq. applies to this Contract, the rates of wages and fringe benefits to be paid to each class of construction mechanic (as defined in MCL 408.1101 (b)) by Contractor and subcontractors must not be less than the wage and fringe benefit rates prevailing in the locality in which the work is performed.

51. 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.

52. 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, 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 elects to and does in fact continue to perform all of its obligations under this Contract.

53. 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

54. 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.

55. 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. PURPOSE

Contractor will provide a Contractor Hosted **Enterprise Freedom of Information Act (FOIA)** Software Solution and applicable Services per the requirements detailed in this Contract. The initial project will consist of creating a configuration for the Michigan State Police, which is expected to be more complex than most, and a standard configuration template that can be replicated and used by most agencies. Contractor acknowledges and agrees that the State will have the right to offer this as a rated service to both State agency business units as well as to local governments pursuant to State law. Contractor will nevertheless have the right to offer these services to MiDeal members, effectively giving local governments two ways to purchase these services.

2. IT ENVIRONMENT RESPONSIBILITIES

For a 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 Matrix	**Name all contractor(s) and/or subcontractor(s) including IT service providers for each contract component.**
Facilities	AWS FedRAMP IaaS
Infrastructure	AWS FedRAMP IaaS
Platform	AWS FedRAMP IaaS
Application	Armedia (ArkCase), Veritone (Redact)
Storage	AWS S3, AWS RDS
Backup	AWS S3, Glacier
Development	Armedia

3. 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.

4. USER TYPE AND CAPACITY

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

Type of User	Access Type	Function	Number of Users	Number of Concurrent Users
Public Citizen	Read & Write	Submit FOIA requests. Receive documents and communications	Scalable	Scalable
State Employee: SOM Security Administrator	Read, Write & Admin	Can add/remove users, change user roles, run security reports. Cannot do anything else in the application (ex: cannot process FOIA requests	6	3
State Employee: SOM FOIA Administrator	Read, Write & Admin	Can edit template and some settings, edit user role functions, and run security reports. Cannot do anything else in the application (ex: cannot process FOIA requests	30	15
State Employee: General End User	Read & Write	Performs all FOIA business activities	60	30

5. 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.

Contractor will configure the solution to integrate with MILogin. Integration with LDAP and Active Directory will be supported out of the box with minimal configuration. The solution will provide role-based access controls. Configuring the access control policies would be the responsibility of the State's designated system administrator based on the instructions in the User and Administrator guides. Contractor will set up default roles and groups during the implementation.

6. REQUIRED FUNCTIONALITY RELATING TO DATA RETENTION, DISPOSAL, AND RETRIEVAL

The State has legal obligations to retain, dispose, and retrieve State Data along with obligations to manage and secure State Data. To meet these obligations, the Solution must allow the State to do the following at no additional cost:

- retain all data for the entire length of the Contract.
- delete its data or request the deletion of its data, even data that may be stored offline or in backups.
- transfer its data back to the State or to a new vendor or new solution.
- transfer its data to the Archives of Michigan as may be required by a retention and disposal schedule.
- retrieve data, even data that may be stored offline or in backups.

Except as otherwise stated in the Contract, Contractor will not dispose of, delete, or destroy State Data without the prior written approval of the State.

7. 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.

8. SOFTWARE

Contractor will provide ArkCase FOIA, an enterprise platform to meet the FOIA and case management requirements listed in the State statement of work. Contractor's case management solution provides out-of-the-box workflow modules that will be implemented in collaboration with

the State using an Agile Scrum methodology with demonstrations of progress at the close of each sprint. Through REST APIs, the solution will expose the core services as standard features that include, but are not limited to:

- Request management / Case management
- Document management
- Correspondence management
- Automated redaction and annotation with exemption codes
- Request and document de-duplication
- Workflow automation
- Audio and video redaction
- Security and access control
- Database management
- Admin, user account and profile management
- Auditing, reporting and analytics to include predictive analytics.
- Customer relationship management (i.e., people and organizations)
- Communications, alerts, and notification management.

ArkCase is an enterprise platform. The following components are integrated into ArkCase:

- PDFTron – embedded online document viewer (third-party component)
- Pentaho Business Analytics Suite – reporting and analytics (third-party component)
- Flowable – BPMN 2.0 workflow engine (open-source component)
- ActiveMQ – leading messaging system (open-source component)

Contractor uses the following frameworks and programming languages in the development of ArkCase:

- Angular – UI framework
- Spring – MVC framework
- Java – programming language
- Kubernetes – containerization framework

Contractor's Solution must meet the requirements 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 least 30 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.

9. INTEGRATION

MiLogin
Contractor must integrate the solution with the State's MiLogin solution to support federation via SAML, OpenID or OAuth federated identity protocols. See Access Control and Authentication section above.

CEPAS
Contractor must integrate the solution with the State's CEPAS system to enable payment processing.

10. MIGRATION

Data migration services are not currently required. The State reserves the right to request such services in the future.

11. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and operational handoff. The Contractor will train SOM Security Administrators, SOM FOIA Administrators, and General End Users to perform the functions described above. Training may be a combination of in-person, online and/or classes in the SOM learning center. Contractor will train 2 or 3 administrators for RMS and at least two people for each department choosing to use the system.

Contractor will deliver a mix of formal and informal training to maximize adoption of the FOIA solution, minimize implementation risk, prepare the organization for day-one capability, and deliver long-term solution sustainability. Contractor's Training Team will deploy training sessions and materials that are integrated with the broader communication and engagement program and conducted in a training environment that replicates the new State FOIA system. This will provide employees with the context and understanding to execute new business processes and systems. Contractor will provide diverse learning vehicles and methods to accelerate the learning curve, increase commitment to new behaviors, skills, capabilities, and knowledge, and lower cost. Learning will not be a one-time event but a continuous process, continuously learning from each training release and improving the next release. The table below provides the key tasks in the training program.

Contractor will provide End-User Training as either a full-day (8-hour) session or divided into shorter 4-hour segments, at the State's option, to enable State staff to learn how to manage and process FOIA requests throughout the entire FOIA process lifecycle. Administrator training will equip participants with the knowledge and skills needed to effectively configure, manage, and maintain the application. Each participant is recommended to attend only one full-day training session. Sessions are further structured into 45-minute modules, each focusing on a specific topic.

Key Tasks	Description

Prepare Guided Training Materials	Contractor will prepare guided training materials on specific topics that cover day-to-day topics.
Provide Employee Training	Contractor will provide in-person, online and/or classes, instructor-led hands-on training for State power users on a replica production system prior to Go-live to ensure State users have the knowledge and tools to perform their duties.
Train Administrator Training	Contractor will train State administrators: administration and configuration training, generating/creating ad-hoc reports, modifying/developing custom correspondence templates for agency use. Armedia will work with State to build a comprehensive curriculum that covers all the functional business areas for the administrative team.
Design Training Materials and Documentation	Contractor will design the training materials, exercises, self-paced training videos, product and training manuals, instructional on-demand videos covering specific topics that cover day-to-day topics for the State.
Survey for Effectiveness	Contractor will survey training participants to compile feedback into lessons learned for incorporation into training updates prior to go-live.

12. 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. 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 life 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.

Contractor will deliver comprehensive documentation to meet State requirements, including user manuals, technical manuals and any other instructional or reference materials necessary to support the software solution. As part of the implementation process, Contractor will develop and submit complete, accurate solution documentation for State review and approval to ensure alignment with State expectations and operational needs before the solution is fully deployed. If any discrepancies, omissions, or errors are identified in the documentation, Contractor will promptly update and redistribute, ensuring that all materials remain accurate and current throughout the life of the contract. Contractor's documentation management approach will guarantee that users always have access to the most up-to-date guidance, reflecting any enhancements, patches, or configuration changes made during the contract term.

Contractor will provide user documentation that offers detailed explanations of software features and functionality, enabling State users to quickly understand and apply the system's capabilities. Contractor will include step-by-step instructions, supplemented with screenshots and examples, to guide users through common processes and resolve typical questions or issues without requiring formal support requests.

13. CONTRACTOR 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.

Contractor
James Bailey 8221 Old Courthouse Rd, Suite 300 Vienna, VA 22182 213-925-2584 james.bailey@armedia.com

14. CONTRACTOR KEY PERSONNEL

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.

Contractor
John Shinnick 8221 Old Courthouse Rd. Suite 300 Vienna, VA 22182 678-596-7775 jshinnick@armedia.com

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.

Contractor
Sanija Shabani 8221 Old Courthouse Rd Suite 300 Vienna, VA 22182 (770) 601-6888 sanija.shabani@armedia.com

15. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks. Contractor must present certifications evidencing satisfactory ICHAT and drug test results for all staff 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 all staff 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 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 all costs associated with ensuring its staff meet all requirements.

Contractor must 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 certification to the State Program Manager(s) that Contractor Personnel's access to State Data has been terminated. Contractor must notify the State in advance of allocating Contractor Personnel to multiple State Contracts or Projects. Contractor must provide detail of how a given Contractor Personnel meets the resource experience requirements in advance of replacing a Contractor Personnel. Contractor must provide monthly summary of Contractor Personnel allocation for all Contractor Personnel who have access to State Data.

Contractor must seek approval from 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 Permitted Subcontractors. If the Contractor intends to utilize Permitted Subcontractors (including but not limited to cloud providers, managed security providers, staff augmentation, etc.) as defined in the Software Terms, the Contractor must 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 Solution.
- The relationship of the Subcontractor to the Contractor. Of the total bid, the price of the Subcontractor's work. Whether the Contractor has a previous working experience with the Subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Solution that will be performed or provided by the subcontractor.

Contractor will use the following Subcontractors:

The legal business name, address, telephone number of the Permitted Subcontractor(s).	**Amazon Web Services, Inc. (AWS)** 410 Terry Ave N Seattle, WA 98109 888-280-4331
A description of Permitted Subcontractor's organization and the Services and/or Deliverables it will provide.	AWS is a global cloud services provider offering infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and managed services. For this contract, AWS will provide cloud hosting, storage, virtual server environments, and related cloud management and security services.
The relationship of the Permitted Subcontractor to the Bidder.	AWS is a Subcontractor providing cloud infrastructure to Contractor for delivery of ArkCase FOIA.
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	• Provision of cloud infrastructure for application hosting and storage management • Managed services for server maintenance, backups, and updates • Security and compliance support (FedRAMP-authorized environment) • Monitoring, logging, and performance optimization • Scalability support to meet user demand spikes

The legal business name, address, telephone number of the Permitted Subcontractor(s).	**Veritone, Inc.** 5291 California Avenue, Suite 350 Irvine, CA. 92617 714-273-3942
A description of Permitted Subcontractor's organization and the Services and/or Deliverables it will provide.	Integration with ArkCase for automated redaction of audio and video content.
The relationship of the Permitted Subcontractor to the Bidder.	Technology partner
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	Armedia will maintain the integration with Veritone which provides a FedRAMP SaaS offering for redacting rich media content.

16. STATE RESOURCES

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

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
Jarrod Barron BarronJ1@michigan.gov 517-249-0406

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

DTMB Program Manager
Jibu John johnj@michigan.gov 517-242-4260

Agency Program Manager
Brice Sample sampleb@michigan.gov 517-335-9450

17. MEETINGS

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 must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

Contractor will also schedule and facilitate additional meetings to support the agile delivery approach, specifically Sprint Planning and Sprint Demonstrations. Sprint Planning sessions, conducted at the start of each sprint cycle, will bring together the State's stakeholders, product owners, and the development team to prioritize backlog items, define sprint goals, and confirm acceptance criteria for planned work. Sprint Demonstrations, held at the end of each sprint, will provide an interactive forum to showcase completed functionality, gather feedback from State participants, and ensure alignment with business needs before the next sprint begins. These agile ceremonies will operate alongside the required weekly and monthly meetings to promote transparency, iterative value delivery, and continuous improvement throughout the project lifecycle.

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 Milestone schedule and associated deliverables are set forth below:

Milestone Event	Associated Milestone Deliverable(s)	Schedule
Project Planning	Project Kickoff	Contract Execution + 10 calendar 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 that are 1) within the scope of the RFP and 2) for any products for which the Contractor is not the publisher of the services or products, Contractor agrees that all such third party services and/or product providers/publishers will be named Permitted Subcontractors under this Contract, and all terms will flow down through Contractor to each Permitted Subcontractor to be responsible for all Terms and Conditions and Schedules regarding the provision of the Solution including, but not limited to, the security obligations as outlined in the Data Security Schedule and Section 21 of the Terms and Conditions.

SCHEDULE A, ATTACHMENT 1 – BUSINESS SPECIFICATION WORKSHEET

Business Specification Number	Business Specification	Current Capability	Requires Configuration	Requires Customization	How Contractor will deliver Business Specification
	REQUIRED SPECIFICATIONS **SECTION 1: COMPLIANCE WITH STATE GUIDELINES AND IT POLICIES**				
1	The solution must integrate with MILogin for public, external users, and internal SOM users.		Y		ArkCase integrates with many authentication systems to inlcude OAUTH, Login.gov as well as supports SAML and SSO. We'll integrate ArkCase LDAP to use MILogin
2	The solution must allow for online submittal of FOIA requests. It must include functionality for task generation to retrieve records from other worksites, invoicing, redaction, document production tracking, in-solution communication, reporting, and searching.	Y			ArkCase provides out-of-the-box collaborative workflows to manage FOIA requests from submission to completion. This includes task management, correspondence management, queue-based workflow, reporting, search and more.
3	The solution must integrate with the State's Centralized Electronic Payment Authorization System (CEPAS) for processing of credit card payments.			Y	ArkCase supports payment processors through it's billable module. We will integrate ArkCase with CEPAS as we have done with other FOIA implementation -- Touchnet, pay.gov, etc..
4	The solution must be fully functional upon installation, allowing the SOM staff to configure the features without procuring the services of the others (the vendor or other technical specialists).		Y		ArkCase is delivered as a fully functional, out-of-the-box solution that is ready for use upon installation. The system is designed with configurable features and administrative tools that allow SOM staff to tailor labels, drop downs, FOIA Due Dates, notifications, and RBAC without requiring additional vendor services or specialized technical resources.
	REQUIRED SPECIFICATIONS **SECTION 2: FOIA ONLINE REQUEST SUBMISSION**				
5	The solution must allow FOIA requestors to submit a FOIA request through an online FOIA interface.	Y			ArkCase fully supports the requirement by providing a secure and intuitive online FOIA request portal that enables members of the public to submit FOIA requests electronically. The portal is accessible from any modern web browser and guides requestors through a structured submission process that captures all required information, including contact details, request descriptions, and any supporting attachments.
6	The solution must allow SOM staff to enter a FOIA request when a FOIA request is received from outside the application (such as US Mail, inter-departmental mail, hand delivered, etc.).	Y			SOM staff can create a manual requests directly in the application. SOM staff can capture all relevant request details, attach supporting documents, and assign the request to the appropriate department, to process the request within the system regardless of the submission method.
7	The solution must require FOIA requestors to select a FOIA request category from a configurable menu.	Y			These are provided through a configurable lookup table. Data field which needs control, restricting values, can be added to the system.
8	The solution must allow FOIA requestors to assign a FOIA request to a SOM business area based on a configurable menu of SOM agencies, categories, or functions.	Y			ArkCase supports both manual or automatic assignments to departments or groups upon a request creation.
9	The solution must allow SOM staff to assign a FOIA request to an SOM business area based on a configurable list of SOM agencies, categories, or functions.	Y			ArkCase enables SOM staff to easily reassign FOIA requests and associated subtasks across business areas while maintaining full audit history
10	The solution must allow SOM staff to reassign a FOIA request and subtasks in and out of SOM business areas with notes and/or instructions, as needed, throughout the workflow.	Y			ArkCase enables SOM staff to reassign FOIA requests and any associated subtasks across business areas at any point in the workflow. Staff can include notes and instructions during reassignment to ensure clear communication and continuity, while all actions are tracked in the system's audit history for accountability and transparency.
11	The solution must allow SOM staff to assign the subtasks of a FOIA request to other SOM staff with necessary notes and/or instructions throughout the workflow.	Y			ArkCase allows SOM staff to assign subtasks of a FOIA request to other staff members at any point in the workflow.
12	The solution must timestamp all FOIA requests.	Y			All requests have create, perfected and update timestamps. Transactions performed during processing are logged and timestamped, providing history from start to finish.
13	The solution must not allow requestors to access or query requests submitted by other requestors.	Y			Through the public portal, requestors only have access to their requests unless the SOM decides to make public the results of a request.
	REQUIRED SPECIFICATIONS **SECTION 3: REQUEST IDENTIFICATION**				
14	The solution must have an automatic generated numbering system for unique identification of all FOIA requests, subtasks, and appeals.	Y			ArkCase supports automatic numbering for requests that is fully configurable in the system.
15	The solution must allow a requestor to have multiple active FOIA requests in process at the same time.	Y			ArkCase does not have any limitations on how many active FOIA requests requesters can have at any given time.

16	The solution must allow multiple requests from the same requestor to be aggregated under the same FOIA account.	Y			ArkCase creates a unique requestor profile that tracks all FOIA requests submitted by that individual. The system imposes no limits on the number of requests a requestor may submit. Within ArkCase, all active and historical requests for a user is display by selecting the Request node under the User.
17	The solution must allow a FOIA request to be separated into multiple subtasks but remain trackable under the original FOIA request.	Y			ArkCase allows a FOIA request to be divided into multiple tasks, enabling different aspects of the request, such as document review, redaction, or research, to be assigned and managed independently. Each subtask remains linked to the original FOIA request, ensuring that all activity, progress, and updates are fully trackable within a single, unified request record.
18	The solution must allow SOM employees to be assigned configurable roles, based upon their duties to respond to FOIA requests, such as FOIA Coordinators, Subject Matter Experts (SMEs), etc.	Y			ArkCase provides RBAC to manage functional access and privileges.
	REQUIRED SPECIFICATIONS **SECTION 4: CALCULATION OF FEES**				
19	The solution must calculate and record the calculation steps of an estimated FOIA request fee.			Y	When provided the States business rules for calculation, Armedia will implement an admin page to manage the rules for auto-calculation of estimated request fees.
20	The solution must calculate and record the calculation steps of the actual FOIA request fee.	Y			ArkCase's Time and Billing Module tracks and calculates the time spent on each FOIA request, providing accurate and auditable records for fee estimation, payment and reporting.
21	The solution must allow the FOIA requestor to request a fee discount or exemption and provide a justification for the discount or exemption, including providing a configurable menu of justifications and a free text box.	Y			ArkCase supports fee discounts with documented justification and includes a free-text field for requestors to provide additional explanation for any reduced fees
22	The solution must allow the ability to override an actual or estimated fee calculation for exemptions.	Y			The Billing module supports override of any fee calculations or exemptions.
23	The solution must allow SOM users to configure and edit the calculation of fees themself, without vendor action.	Y			ArkCase's Time and Billing module is configurable, allowing SOM users to define and modify charge roles at any time to align with agency policies and workflows.
24	The solution must allow SOM users to manually enter the payment amount and type received from different sources for payments that were received outside of the system, such as through cash and checks (EX: $40 FOIA request fee was paid for via $25 in cash and $15 from check #1277).	Y			ArkCase allows SOM users to manually record payments received outside the system, including cash, checks, or other payment types. Users can enter the payment amount and specify the source of each portion. ensuring accurate tracking and reconciliation of all FOIA-related fees.
25	The solution must allow the SOM users to view a standard list of costs, such as hourly wages, applicable to responding to a FOIA request.		Y		ArkCase provides the ability to configure charge roles and associated rates for each role.
26	The solution must allow SOM users to calculate agency-indicated fringe benefit percentage charges for responding to the request.			Y	ArkCase enables SOM users to calculate and apply agency-specified fringe benefit percentage charges when processing FOIA requests. This functionality ensures that all applicable costs are accurately captured and incorporated into the overall fee calculation.
27	The solution must be able to generate an itemized invoice including the fee categories for the requestor.		Y		ArkCase can generate itemized invoices for FOIA requestors that clearly break down all applicable fee categories, including search, review, duplication, and any other charges. Invoices are generated using a built-in correspondence template that can be modified.
	REQUIRED SPECIFICATIONS **SECTION 5: IN-SOLUTION COMMUNICATION**				
28	The solution must allow only SOM staff with specified user roles to communicate with FOIA requestors via both configurable automated and manually initiated emails. This includes requests for clarification.	Y			Emails can be generated directly from ArkCase. Internally, ArkCase tracks and logs emails sent from within the system. If sent from an email application, the user can still export the email and save it to ArkCase.
29	The solution must be able to send configurable alerts, notifications, and reminders throughout the workflow (different stages/steps of workflow) at certain triggers.	Y			ArkCase has a built in notification system that uses both emails and dashboard notifications. These can be triggered by the workflow or through system wide alerts when FOIA requests meet the trigger threshhold (ie. A request that has not had any action for a period of time)
	OPTIONAL SPECIFICATIONS **SECTION 5: IN-SOLUTION COMMUNICATION**				
30	The solution should allow SOM staff to communicate with other SOM staff throughout the workflow (different stages/steps of the workflow) with a chat functionality. These communications must be reportable.	Y			ArkCase provides a notes section for chat threads and users can be identified in the note using the @JohnDoe which will send John Doe an email of the note. ArkCase integrates with O365, so we could integrate with Microsoft Teams for chat as an enhancement.
	REQUIRED SPECIFICATIONS **SECTION 6: FOIA TEMPLATES**				

31	The solution must provide configurable templates that may be used for automated and manual electronic correspondence with requestors.	Y			These are provided by the Correspondence Module which can auto-populate forms and letters.
32	The solution must allow only SOM users in the appropriate role to configure, change, format, and edit template language and content, and without requiring vendor action.	Y			ArkCase leverages role-based access control (RBAC) to ensure that only authorized SOM users can modify system components such as correspondence templates, FOIA configurations, and other critical settings. The State retains full control over permissions, enabling it to restrict system changes to designated users.
33	The solution must provide templates that use common assets, changeable by SOM users in the appropriate role to configure without vendor action, for common template sections (such as letterhead) so that a change to the common asset changes the appearance of all templates that use that common asset.	Y			Supported OOTB.Refer to H32.
34	The solution must have configurable autofill templates with required fields such as FOIA number, fees, requestor name, address, email address, etc.	Y			ArkCase correspondence templates utilize merge fields that automatically populate key information, such as FOIA number, fees, requester name, address, and email, when creating tempaltes. Additional fields can be added to templates as needed.
	REQUIRED SPECIFICATIONS **SECTION 7: TRACKING, SEARCHING, SORTING, AND PRIORITIZING OF FOIA REQUEST AND APPEAL**				
35	The solution must allow SOM staff to process appeals, although appeals will be received outside of system.	Y			These features are provided by the core ArkCase product and available through the main system based on the users functional access rights (RBAC).
36	The solution must allow SOM staff to track the status of an appeal.	Y			Supported OOTB
37	The solution must allow SOM staff to track the status and progress of a FOIA request throughout the workflow.	Y			ArkCase tracks FOIA requests through all stages of the workflow, including intake, fulfillment, approval, and other defined states. SOM users can easily view the current state of any request in real time, providing clear visibility into its progress throughout the process.
38	The solution must allow SOM staff to override or change the status of FOIA requests and appeals.	Y			SOM users have the ability to change a status request or an appeal OOTB.
39	The solution must allow SOM staff to categorize, search and track FOIA requests, appeals, high profile requests, and media requests.	Y			ArkCase configurable filters, tags, and search capabilities ensure that all request types can be efficiently managed and monitored throughout the workflow.
40	The solution must allow SOM staff to flag, prioritize, or escalate a FOIA request according to configurable categories.	Y			ArkCase enables SOM staff to flag, prioritize, or escalate FOIA requests using configurable categories and business rules. Examples include placing requests on hold, applying statutory extensions, routing through approval workflows, and other actions to ensure proper handling of each request.
41	The solution must allow SOM staff to flag requestors according to configurable categories.	Y			Supported OOTB
42	The solution must allow SOM staff to search and sort FOIA requests according to configurable categories (such as by date, requestor, SOM staff, SOM agency, current status, FOIA #, priority, flag, extensions).	Y			ArkCase provides a comprehensive search function that indexes both metadata and content, providing full text search or metadata based search. The search results are also controlled by RBAC and Access Control Lists (ACL). Results can be filtered and sorted to narrow the results.
43	The solution must calculate deadlines and due dates, and allow SOM staff with appropriate permissions to change those dates (extensions, SOM holidays) according to configurable categories.	Y			ArkCase's configurable FOIA settings enable SOM users to calculate deadlines, due dates, and extensions accurately. The system automatically accounts for holidays and work schedules to ensure compliance with statutory timelines.
	OPTIONAL SPECIFICATIONS **SECTION 7: TRACKING, SEARCHING, SORTING, AND PRIORITIZING OF FOIA REQUEST AND APPEAL**				
44	The solution should provide allow FOIA requestors to track the status of their FOIA request.	Y			Registered users are able to track their request through the public portal.
	REQUIRED SPECIFICATIONS **SECTION 8: REDACTION**				
45	The solution must allow manual redaction of information.	Y			ArkCase provides both manual and auto-redaction based on patterns.
46	The solution must allow SOM users to configure and edit, without vendor action, a list of redaction reasons (such as statutory citations).	Y			Users with administrative access can adjust this list.
47	The solution must be capable of retaining the original unredacted version of any FOIA records and create and retain a separate redacted copy of the record.	Y			The original document is saved as the original version with higher access controls than the redacted versions.
48	The solution must ensure that the redactions cannot be removed, and that confidential or restricted information cannot be revealed, from the separate redacted copy of the record.	Y			Once burned in, redactions cannot be removed. Only the original document can be used to retrieve redacted values.

49	The solution must require SOM users to select a redaction reason (statutory citation) for any redaction made and tie it to the redaction and add comments if desired.	Y			ArkCase requires SOM users to select a redaction reason for each redaction, including the applicable statutory exemption code. The system ties the exemption code to the redaction and allows users to add optional comments, ensuring auditability for all redaction actions.
50	The solution must allow an ability to cite specific FOIA statute, and additional comments if required, to tie to a redacted item as part of redaction functionality.	Y			Supported OOTB
	OPTIONAL SPECIFICATIONS **SECTION 8: REDACTION**				
51	The solution should allow the SOM staff to configure pattern recognition to automatically identify certain types of information for possible redaction (such as telephone numbers, Social Security numbers, credit card numbers).	Y			ArkCase provides a configurable list of patterns for auto-redaction with the ability to select the appropriate redaction code(s) for each pattern.
52	The solution should allow editing or redaction of multimedia information (such as audio and video files).	Y			ArkCase integrates with Veritone for audio and video redaction.
	REQUIRED SPECIFICATIONS **SECTION 9: REPORTS**				
53	The solution must have a reporting function.	Y			ArkCase provides canned reports and adhoc reports using Pentaho Reporting tool to create and produce reports. ArkCase provides the reports which are required by FOIA policies as part of the base product.
54	The solution must support up to 25 canned reports with the initial implementation.	Y			We provide 32 OOTB reports required for federal FOIA.
55	The solution's report functionality must include, but not be limited to, filters, sort order, ability to schedule reports to run automatically, and changes to date ranges.	Y			Reports can be filtered and sorted by any of the fields/metadata in the report.
56	The solution must allow for the creation of configurable ad-hoc reports and be able to save the ad-hoc report's search parameters for future re-use.	Y			Users with the necessary access/authorization can create reports and publish them publically or privately.
57	The solution must be able to present the report information through different views such as data views and statistical views (including, but not limited to, bar chart, pie chart, column chart, etc.)	Y			Reports can be viewed in a variety of formats. Data can be exported to other tools for statistical analysis.
58	The solution must allow reports to be configured, managed, and controlled by appropriate SOM user roles.	Y			Reports can also be restricted based on user access rights.
59	The solution must provide reports to assist with monitoring the use, security, and functionality of the system, including but not limited to, reports of all users in the system, their role in the system, and whether their account is active or disabled (and date(s) the account was activated and/or disabled), daily payment transaction reports, CEPAS reports, refund reconciliation reports, date of last login reports for all users, daily audit trail of activity by users, and audit reports.		Y		ArkCase provides a reporting capability based on Pentaho Business Analytics Suite. Data fields within the database can be exposed to static and analytical reports. As part of the implementation, Armedia will training SOM staff on the capabilities of the ad-hoc reporting so SOM staff can create reports as needed.
60	The solution must be able to schedule the generation of reports according to SOM user-configurable conditions.	Y			Reports can be scheduled to run as scheduled jobs and the ability to auto-distribute.
61	The solution must be able to export reports to Excel and PDF formats.	Y			Additionally, the data can be exported in its raw form.
62	The solution must allow downloading, viewing, as well as sending the reports electronically to certain recipients, teams, and groups.	Y			These can be schedule to run on schedule and route reports automatically to a distribution group.
63	The solution must allow the generation of reports using all the modules of application at the same time.	Y			Reports can use data from modules as the system uses a single database. Results from search module can also be incorported into the reports.
	OPTIONAL SPECIFICATIONS **SECTION 9: REPORTS**				
64	The solution reporting tool should have user-configurable automated generation and electronic sending of reports or notifications.	Y			Reports can use data from modules as the system uses a single database. Results from search module can also be incorported into the reports.
	REQUIRED SPECIFICATIONS **SECTION 10: SECURITY - EXTERNAL HOSTING ONLY**				
65	The solution must include contiguous SOC 2 Type II compliance for the five AICPA Trust Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.	Y			Armedia proposes a FedRAMP Moderate solution which encompasses the SOC 2 Type II compliance requirements.
66	The vendor must provide a SOC 2 Type II report for the Application and SOC 2 Type II report for Hosting for the five AICPA Trust Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. The vendor must be able to provide contiguous SOC reports covering the entire year. (COTS and SaaS)	Y			Armedia proposes a FedRAMP Moderate solution which encompasses the SOC 2 Type II compliance requirements.
67	The vendor must provide AICPA Complementary User Entity controls that are used by vendor for any sub-service organizations used (AWS, Azure, etc.), as defined in the SOC report.	Y			Armedia proposes a FedRAMP Moderate solution which encompasses the SOC 2 Type II compliance requirements. Our FedRAMP solution is hosted within the AWS FedRAMP IaaS.
68	The vendor must provide a list of all sub-service organization products used to host, maintain, or build the application.	Y			The proposed solution runs within AWS FedRAMP IaaS.
69	The solution must hosted data (including test, production, backup, and recovery data) in the United States only.	Y			Reports can use data from all modules as the system uses a single database. Results from search module can also be incorported into the reports.
70	The solution must host data in a FedRAMP moderate authorized environment.	Y			ArkCase is a FedRAMP Authorized

71	The solution must store data in a government cloud environment (as opposed to commercial cloud), if one exists.	Y			All data is stored in the FedRAMP moderate cloud.
72	The vendor must list the technologies in place to prevent DDOS attacks.	Y			AWS provides AWS Shield as part of the infrastructure offering. On top of that, AWS Web Application Firewall (WAF) provides additional protection against DDOS.
73	The vendor must list the types of managed interfaces (firewalls, routers, subnets, etc.) that protect the boundary of the application.	Y			We use AWS WAF in front of load balancers (ALBs). We use Virtual Private Clouds for each application. ArkCase FOIA and Portal user-based inbound traffic comes through ALBs. Within VPCs, we use Security Groups and Network Access Control Lists (NACLs). We used Software Defined Networking (SDN) within Elastic Kubernetes Services (EKS) to implement policies that confine internal traffice to only what is permitted.
74	The solution must detect attacks and indicators of potential attacks in accordance with Michigan Security Operations Center (MiSOC) monitoring standards and procedures.	Y			The control and security protections implemented on top of AWS FedRAMP moderate features cover the requirements of MiSOC. Armedia can assist the State in testing and validating compliance.
75	The vendor must scan hosted services for vulnerabilities every month. A report of the scan results and the name of the tool used should be provided to SOM each month. Vulnerability scan report and results must meet SOM SADLC requirements.	Y			Automated scans using Tenable/Nessus are executed bi-weekly on servers, containers and databases. The scan reports and results are uploaded to max.gov to meet SOM SADLC requirements. Additionally, Splunk is used to monitor all activity to the servers which is also protected by multi-factor authentication. The State can review these reports directly from MAX.gov.
76	The vendor's vulnerability scanning tool must be updated before each scan.	Y			Tenable/Nessus is updated based on the vendors required patching/upgrade schedule. Splunk is updated on the vendors required patching schedule.
77	The vendor must permit Michigan Cyber Security scan the application for vulnerabilities.	Y			This can be arranged and coordinated with Armedia to insure that no AWS or Armedia cybersecurity policies are violated if tools need to be placed in the environment. Michigan Cyber Security can perform tests directly against the application to check for vulnerabilities but must coordinate with the State as to the impact it may cause.
78	The vendor must provide to SOM evidence that security patches are up to date.	Y			The scan reports produced by Tenable/Nessus are designed to check and report on mandatory patches, upgrades and security vulnerabilities. These monthly reports are available through MAX.gov.
	REQUIRED SPECIFICATIONS **SECTION 11: SECURITY**				
79	The solution must allow for the creation of multiple SOM user roles with varied (configurable) system access and capabilities.	Y			There is no limit to the roles that can be configured
80	The solution must support the creation of user groups by agency, so users cannot access requests/responses of other agencies.	Y			There is no limit to the roles that can be configured
81	The solution must allow for the creation of an administrator role that does not have the security-related capabilities assigned to the Security Administrator role.		Y		Administrators can be assigned with specific roles as to what they can modify or monitor in the application. Administrators can also be relegated to specific set of groups and data.
82	The solution must allow for a separate Security Administrator that does not have the system-related capabilities assigned to the Administrator role or any other role in the system.		Y		System administrators have the highest level of access to manage system features directly in the application. Security can be managed by System Administrators at the appliation level. Overall management of security of the environment is provided by the Cloud Security engineer.
83	The solution must allow for the disabling or deletion of any single system administrator role that would have access to both system and security related capabilities.		Y		This can be managed through roles. There are separate roles/groups for System Administrators, Site administrators and application administrators.
84	The solution will not store credit card information.	Y			ArkCase does not store credit card information.
85	The solution must support the following system roles: A. SOM Security Administrator (can to add/remove users, can to change user roles, can run security reports, cannot do anything else in the application (*ex: cannot process FOIA requests*). B. SOM Administrator (can edit template and some settings, can edit user role functions, can run security reports, cannot do anything else in the application (*ex: cannot process FOIA requests*). **C. No "all powerful" system administrator user role**		Y		System security will be the responsibility of a designated staff member and Armedia staff who will monitor the overall cloud infrastructure, logging and cybersecurity of the environment. ArkCase has it's own administrators wo can manage application level configuration and certain security features, such as role management and access controls. These are all separate roles at different levels.
86	The vendor must follow the SUITE process and assist with the system security plan (SSP) process managed with the State's Governance Risk and Compliance Tool (Keylight) (SA-02).	Y			Armedia has undergone multiple security assessments and will provide support as well as documentation which should expedite the process. The State can use our SSP as a basis if needed for interal use.
87	The vendor must document the maintenance plan, including their request, approval, and recordkeeping methodology (MA-02).	Y			Armedia can provide our Maintenance Procedure document which covers this control.

88	The solution must automatically disable inactive user accounts after 60 days and system accounts after 365 days.		Y		ArkCase integrates with SOM directory services for password and authentication policies. ArkCase, by default, implements a 90 day no-use period before deactivating an account which can be configured to State specifications. System accounts for the SaaS are specific to Armedia but IAM roles can be set up with controlled access for State designated administrators if needed. These accounts also follow a 90 day
89	The solution must automatically document account creation, modification, disabling, and removal actions.	Y			All account level activity is logged and auditable.
90	The solution must enforce a limit of three invalid logon attempts within a defined time period during a user session upon which the account or node is automatically locked for a minimum period of 30 minutes, or until released by an administrator.	Y			ArkCase integrates with SOM directory services for password and authentication policies. ArkCase, by default, implements five invalid login lockout with five minute no access. Both can be configured to the State's requirements.
91	The solution must display a customizable message or warning banner before granting access to the system.		Y		This is configured for each system with verbiage provided by the customer.
92	The solution must initiate a session lock after a configured number of minutes of inactivity. The solution session lock, when activated, must place a publicly viewable pattern onto the associated display, concealing what was previously visible on the screen.	Y			ArkCase defaults this to 30 minutes which can be configured.
93	The solution must be able to generate an audit of the following events: user account management activities; creation, modification, or deletion of accounts; and use of Administrator privileges.	Y			ArkCase logs these transactions and reports can be produced by users with access.
94	The solution must generate audit records containing: type of event that occurred, when the event occurred, where the event occurred, the frequency or count if the record represents multiple occurrences of the event, source of the event, destination of the event, outcome of the event, and identify of any individuals or subjects associated with the event.	Y			Logs track the event, user, date/time, function executed and data accessed. Reports can be run on the logs by an administrator to detect usage.
95	The solution must provide sufficient audit storage capacity to support ongoing operations and rollback of the system. The solution must send an audit storage alert when capacity is getting low.	Y			ArkCase is deployed to auto-scale up and down to optimize usage and costs. Storage scaling is set at 80% threshold to autoscale when the threshold is hit. This value as well as the incremental increase are configurable and we review growth quarterly to adjust these to optimize costs.
96	The solution must use internal system clocks to generate time stamps for audit records mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and maintains time synchronization within 20 milliseconds of reference clocks.	Y			ArkCase is synchronized through AWS and the system can be configured to synchronize to UTC.
97	The solution, for password-based authentication, must store and transmit only cryptographically-protected passwords, enforce password minimum and maximum lifetime restrictions, prohibit password re-use for a defined set of generations, and support SOM password complexity requirements.	Y			ArkCase integrates with SOM directory services for password and authentication policies. ArkCase supports SAML, oAuth and OIDC. ArkCase support MFA as well. Communication with directory service (i.e., Active Directory) is encrypted.
98	The vendor must provide a description of the functional properties of the security controls to be employed. The vendor must provide design and implementation information for the security controls and application.	Y			Armedia can provide security implemetations, monitoring and other controls. These are all defined in our System Security Plan (SSP) for the FedRAMP enviroment. ARkCse, application level security, will be provided documenting authentication, access controls, logging and other features to ensure system availability and confidentiality.
99	The vendor must provide a comprehensive system configuration manual and technical baseline.	Y			This is provided for the ArkCase application.
100	The vendor must provide evidence of secure coding and use of security engineering principles.	Y			ArkCase uses Veracode as part of its CI/CD pipeline for preemptive identification of potential vulnerabilities. In addition, we use Sonar for static and dynamic code analysis to identify potential issues. The DevSecOps code pipeline and reports can be provided for configuration and customization performed for the State.
101	The vendor must define a written flaw remediation process that includes approval of the change, verification that the change was implemented correctly, and a tracking process.	Y			This is covered under our Program Management approach which will be documented in the Program Management Plan (PMP). We use JIRA for tracking all issues, including change requests, allowing tracking from start to end.

102	The vendor must provide a list of protections in place that prevent unauthorized and unintended information transfer via shared system resources.	Y			ArkCase implements RBAC/ACL controls for functional and data access controls. The system is protected through AWS security features to include GuardDuty, Inspector and WAF. Transactions in the application are logged for all events with the ability to audit down to the data access level. We can set up monitors to detect access that exceeds normal operations but will require information from the State on that volume. We will monitor traffic and access and can use that data over a monthly period to extrapolate a baseline which could be used to identify unauthorized access. For data that is downloaded locally, that must be controlled by the state as ArkCase does not track data outside its controls.
103	The solution must encrypt all data in flight and at rest using 256 AES and TLS 1.2, HTTPS or higher.	Y			Armedia encrypts all data in flight and at rest using 256 AES and TLS 1.2, HTTPS or higher.
104	The vendor must document how encryption keys are managed and protected.	Y			Key management is managed through AWS Key Management Services.
105	The solution must be able to delete data and records in compliance with the SOM's applicable records Retention and Disposal Schedules.		Y		This is provided through the records governance but must be configured based on the SOM's policies and schedules. Armedia will configure these but the SOM can also adjust and manage these policies.
106	The solution must be configurable by SOM to retain and automatically purge records based on SOM approved retention periods, and be able to apply, track, and lift legal holds to the automated deletion process.		Y		This is provided through the records governance but must be configured based on the SOM's policies and schedules. Armedia will configure these but the SOM can also adjust and manage these policies.
107	The solution must not allow the creation of temporary, emergency, or group accounts.		Y		This requires configuration of specific roles and groups which can then be managed by the customer.
108	The solution's vulnerability remediation timeline must be in alignment with SOM Policy remediation requirements.	Y			We follow FedRAMP moderate guidelines as defined in our SSP. We can adjust to meet the SOM's Policy as long as it does not reduce the controls in place.
109	The SOM must be able to receive a copy of the data for records retention storage on premise on request.			Y	When a record reaches it's retention period, the system can be configured to package and send to the customer. On demand requests require manual extraction through the governance management function.
110	The solution must employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.	Y			The system implements FedRAMP moderate controls at all endpoints to ensure external access. ArkCase does not allow downloading of software. That must be managed by the customers. Our DevSecOps software development methodoloyg has mutliple controls to ensure no code is introduced into the system that could compromise its functionality.
111	The solution must employ integrity verification tools to detect unauthorized changes to software, firmware, and information.	Y			Our software development approach and the implementation of DevSecOps automation puts in controls that validate and check code for vulnerabilities before releasing into higher environments. Additionally, only the QA/CM has the ability to promote code. The QA/CM perrforms additinal testing to ensure no vulnerabilities have been introduced, including penetration testing.
112	The solution must check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.		Y		Each form has data validation builit into to ensure data types and data values for the field are enforced, through lookup tables as well as form based controls. Additional logic to validate the entire form can be implemented based on the customers requirements, ensuring data integrity during data entry.
113	The solution must use version control software.	Y			Solution usues version control software manage source code, configuations and related artifacts. These ensure ful traceability of changes, secure audit history and rollback capabilities.
114	The vendor must separate development, testing, and production environments.	Y			Separate development, testing and production environments are maintained to ensure proper seggregation of duties, and reduce the risk of unintended impacts on live systems. We implement DevSecOps to control deployments with automated CI/CD pipelines for both the base ArkCase code and customer specific code.

115	The vendor must list protections that are in place to prevent unauthorized and unintended information transfer via shared system resources.	Y			Armedia enforces strict access controls, data isolation and memory management to prevent unauthorized or unintended information transfer across shared services. Encryption (TLS 1.2/1.3 and AES-256), boundary protections and DLP solutions safeguard data in transit, at rest and during processing. Continuous monitoring, auditing and secure configuration management ensure ongoing compliance and protection against data leakage.
116	The vendor must obtain public key certificates from an approved service provider.	Y			We follow FedRAMP moderate guidelines as defined in our SSP. We can adjust to meet the SOM's Policy as long as it does not reduce the controls in place.
117	The solution must maintain a separate execution domain for each executing process.	Y			Each customer's system is deployed into a their own private space, fully isoloated from other customers. ArkCase does execute separately from the Public portal and other services are containerized, running in their own space.
118	The vendor must provide to SOM its release notes on maintenance activity, patching cycles, and system updates.	Y			We will coordinate with SOM on all releases of the software as defined and controlled by our Project Manager and the Project Schedule. All these artifacts are included in a release, tracked through our JIRA project tracking tool.
119	The vendor must only perform non-local maintenance activities through a SOM VPN, if the solution is internally hosted.	Y			We will coordinate with SOM for any maintenance required within their environment. This is not expected.
	REQUIRED SPECIFICATIONS **SECTION 12: MOBILE APPLICATION**				
120	The solution must have a responsive design to be able to run on mobile platforms.	Y			ArkCase is built on a highly responsive UX.
	REQUIRED SPECIFICATIONS **SECTION 13: DELIVERY TO REQUESTORS**				
121	The solution must allow SOM staff to upload electronic documents in many file formats that are responsive to the request for delivery to the requestor.	Y			There is no restriction on the file types that can be uploaded.
122	The solution must allow the SOM staff with specific user roles only to deliver the documents to the requestor electronically via a secure portal interface, or document the date that the documents were physically mailed to the requestor.	Y			Supported OOTB
123	The solution must allow SOM staff to publish selected FOIA records in a public archive.	Y			ArkCase enables SOM staff to publish selected FOIA records to a public archive, providing a secure and searchable Public Reading Room.
124	The solution must all SOM to configure, edit, and publish its own FAQs and other FOIA information.		Y		Only administrators with the role to publish content can modify these pages. However, the solution provides a workflow to control the review-approve-publish workflow.
125	The solution must allow SOM staff to print responses for fax or US Mail.	Y			Supported directly from within ArkCase
126	The solution must allow SOM staff to electronically export requests and responses to a person who does not have access to the solution.	Y			The State must control requests that are sent outside of ArkCase. ArkCase can create an export package which can be email, printed and mailed or delivered through an alternate path.
127	The solution must allow SOM to certify documents that are provided to requestors.	Y			ArkCase allows SOM staff to certify documents provided to requestors, ensuring that each document is officially verified and authenticated before release. The system tracks certified documents, maintaining a complete and auditable record of all FOIA responses.
	REQUIRED SPECIFICATIONS **SECTION 14: DOCUMENTATION AND TRAINING**				
128	The vendor must provide a digital and editable training plan that covers the types of training, roles of users who should attend which training, training materials provided for each training, and training logistics and needs from the customer.	Y			A training plan will be developed in collaboration with the State. These will be virtual, web-based or in-person as required. Additional training can be added as needed.
129	The vendor must provide training to the SOM trainers (in person or virtually, at SOM discretion) about the software and basic system functionality.	Y			Armedia will plan and coordinate these training sessions as well as provide train-the-trainer type sessions allowing the State to perform future training internally.
130	The vendor must provide administrator training sessions for configuration of the portal and the administration of the instance, with knowledge areas inclusive of the build, configuration, and unit test activity, if needed.	Y			Armedia will plan and coordinate these training sessions as well as provide train-the-trainer type sessions allowing the State to perform future training internally.
131	The vendor must provide recorded training sessions and provide recording videos for future user reference.	Y			We will record virtual training sessions and provide the transcript to the State. We provide training and have content available at https://www.arkcase.com/resources/arkcase-videos/
132	The vendor must provide technical support during regular business hours.	Y			This will be covered under our Service Level Agreement.

133	The vendor must provide all training in a web accessible format at a minimum. Other training formats and methods in addition to the web training are acceptable if they meet SOM operational needs.	Y			Training material will be provided in digital form. It will be available via web downloads. Online, self-paced training will be provided based on State requirements.

SCHEDULE B – PRICING

1. License Fees (Includes Support Service and Hosting Fees). ArkCase License Fees are based on an annual per user subscription model designed as volume-based pricing, meaning the per-user cost decreases as the number of licenses purchased across the State increases. For example, in Year 1 the cost of 150 Contributor licenses would be calculated as shown in the example table below.

Illustrative Example:

Tier	Quantity	Year 1 Per User Cost	Total
ArkCase-USR-FedRAMP Contributor (50)	50	$451.44	$22,572.00
ArkCase-USR-FedRAMP Contributor (51-100)	50	$293.44	$14,672.00
ArkCase-USR-FedRAMP Contributor (101-200)	50	$190.73	$9,536.50
Total			**$46,780.50**

Costs associated with hosting and for ongoing maintenance and support of the Solution (the "**Support Service Fees**") to meet the requirements of **Schedule D - Service Level Agreement** are included in the annual license fees. Contractor may begin invoicing for license fees after installation, configuration, and State testing and acceptance of the Solution and after the State has requested a specific number of user licenses.

2. Implementation Fees.
   a. SOM Enterprise FOIA Platform. Contractor may charge a one-time firm-fixed $378,366.08 fee for all services required to implement the SOM Enterprise FOIA Platform (configuration, customization, integration, testing, etc.). As shown in Table 2 below, Contractor may invoice no more frequently than monthly for deliverables the State has received, tested, and formally approved during the prior month.

Invoicing Schedule by Deliverables:	%	Increments	Increment Fee	Total
Project Management and Monthly Status Report		4	$11,485.60	$45,942.40
Requirements Signoff	10%	1	$33,242.37	$33,242.37
Design	10%	1	$33,242.37	$33,242.37
• Architecture Design (Logical and Security)			$0.00	$0.00
• Interface Control Design			$0.00	$0.00
Implementation Sprints (3)	10%	3	$33,242.37	$99,727.10
User Guide	15%	1	$49,863.55	$49,863.55
User Acceptance Testing	15%	1	$49,863.55	$49,863.55
Go Live	20%	1	$66,484.74	$66,484.74
				$378,366.08

   b. Additional Optional Future Onboarding Implementations. In the event, the State requests additional agency onboarding services, the Onboarding fees listed in Tables 2

and 3 below will apply. For each requested onboarding project, Contractor may charge the associated one-time firm-fixed fee after the State has received, tested, and formally approved any specific onboarding services.

3. Training & Documentation Fees. Contractor may invoice these fees in one lump sum after the State has received, reviewed, and formally approved the training and documentation deliverables.

4. Postproduction Warranty. Contractor must provide a 90 calendar days postproduction warranty at no cost to the State. The postproduction warranty will meet all requirements of the contract, including all Support Services identified in Schedule D.

5. Rate Card for Ancillary Professional Services. The labor rates in Table 5 below apply to optional future services purchased during the life of the contract. Upon request, Contractor will use these rates to provide firm-fixed fee quotes for all services other than the ones listed Tables 2 – 4 below.

6. Additional Pricing Terms. If Contractor reduces its prices, or offers a lower price to any other entity, private or public, for any of the software or services during the term of this Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send a notice to the State's Contract Administrator with the reduced prices within fifteen (15) Business Days of the reduction taking effect.

7. Travel and Expenses. The State will not pay for overtime or travel expenses.

Table 1: Estimated Contract Cost Summary

This table reflects the State's current estimated usage. This is an estimate, not a commitment to purchase.

Base Years 1-5	Est. Cost
Software Licensing (includes Support Fees & Hosting) Estimated from Table 2.	1,898,010.10
Implementation & Onboarding Estimated from Table 2.	462,203.11
Custom Services (Reports, Templates, Portals) Estimated from Table 2.	27,560.27
Base Years Total	**2,387,773.48**
Option Years 6-10	
Software Licensing (includes Support Fees & Hosting) Estimated from Table 3.	4,103,536.37
Implementation & Onboarding Estimated from Table 3.	159,573.62
Custom Services (Reports, Templates, Portals) Estimated from Table 3.	39,335.37
Option Years Total	**4,302,445.36**
ESTIMATED TOTAL	**$6,690,218.84**

Table 2: Software Licensing & Implementation Fees: Years 1-5

Product / Service	Item & Fee Type	Year 1	Year 2	Year 3	Year 4	Year 5	Comments
ArkCase-USR-FedRAMP (50)	Subscription License	$1,504.80	$1,549.94	$1,596.44	$1,644.33	$1,693.66	Annual cost per user
ArkCase-USR-FedRAMP (51-100)	Subscription License	$978.12	$1,007.46	$1,037.68	$1,068.81	$1,100.87	Annual cost per user
ArkCase-USR-FedRAMP (101-200)	Subscription License	$635.78	$654.85	$674.50	$694.74	$715.58	Annual cost per user

ArkCase-USR-FedRAMP (201-300)	Subscription License	$572.20	$589.37	$607.05	$625.26	$644.02	Annual cost per user
ArkCase-USR-FedRAMP (301-500)	Subscription License	$514.98	$530.43	$546.34	$562.73	$579.61	Annual cost per user
ArkCase-USR-FedRAMP (501-1000)	Subscription License	$463.48	$477.39	$491.71	$506.46	$521.65	Annual cost per user
ArkCase-USR-FedRAMP (1001-2000)	Subscription License	$417.13	$429.65	$442.54	$455.82	$469.49	Annual cost per user
ArkCase-USR-FedRAMP (2000 +)	Subscription License	$375.42	$386.68	$398.28	$410.23	$422.54	Annual cost per user
ArkCase-USR-FedRAMP Contributor (50)	Subscription License	$451.44	$464.98	$478.93	$493.30	$508.10	Annual cost per user
ArkCase-USR-FedRAMP Contributor (51-100)	Subscription License	$293.44	$302.24	$311.31	$320.65	$330.27	Annual cost per user
ArkCase-USR-FedRAMP Contributor (101-200)	Subscription License	$190.73	$196.46	$202.35	$208.42	$214.67	Annual cost per user
ArkCase-USR-FedRAMP Contributor (201-300)	Subscription License	$171.66	$176.81	$182.11	$187.57	$193.20	Annual cost per user
ArkCase-USR-FedRAMP Contributor (301-500)	Subscription License	$154.49	$159.13	$163.90	$168.82	$173.88	Annual cost per user
ArkCase-USR-FedRAMP Contributor (501-1000)	Subscription License	$139.04	$143.22	$147.52	$151.95	$156.51	Annual cost per user
ArkCase-USR-FedRAMP Contributor (1001-2000)	Subscription License	$125.14	$128.89	$132.76	$136.74	$140.84	Annual cost per user
ArkCase-USR-FedRAMP Contributor (2000 +)	Subscription License	$112.63	$116.00	$119.48	$123.06	$126.75	Annual cost per user
SOM Enterprise FOIA Platform	One-Time Implementation Fee	$378,366.08	$0.00	$0.00	$0.00	$0.00	One-time setup of the base Enterprise FOIA Platform. Includes $21,342.40 training and $44,273.60 documentation deliverable costs.
Department Large/Complex (separate deployment)	Optional Onboarding Fee, Per Request	$133,640.40	$137,649.61	$141,779.10	$146,032.47	$150,413.44	Separate deployment based on Enterprise FOIA

Department Medium/Large (minor customizations leveraging SOM Enterprise FOIA)	Onboarding Fee, Per Request	$79,052.80	$81,424.38	$83,867.11	$86,383.12	$88,974.61	Leverage Enterprise FOIA. Custom Portal. Up to 3 custom reports and custom templates.
Department Small (no customizations leveraging SOM Enterprise FOIA)	Onboarding Fee, Per Request	$28,359.24	$29,210.02	$30,086.32	$30,988.91	$31,918.58	Leverage existing portal, workflow, reporting. Adding up to 50 users and groups. 2 virtual training sessions.
Custom Report	One-Time Fee, Per Request	$3,750.00	$3,862.50	$3,978.38	$4,097.73	$4,220.66	Up to 10 columns with lookups and calculations,
Custom Correspondence Template	One-Time Fee, Per Request	$1,500.00	$1,545.00	$1,591.35	$1,639.09	$1,688.26	10 fields or less
Custom Portal	One-Time Fee, Per Request	$8,536.00	$8,792.08	$9,055.84	$9,327.52	$9,607.35	Single page custom portal based on existing external portal
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 100 hours	Optional Subscription License	$10,450.00	$10,763.50	$11,086.41	$11,419.00	$11,761.57	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 250 hours	Optional Subscription License	$24,750.00	$25,492.50	$26,257.28	$27,045.00	$27,856.35	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 400 hours	Optional Subscription License	$33,000.00	$33,990.00	$35,009.70	$36,059.99	$37,141.79	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 700 hours	Optional Subscription License	$50,050.00	$51,551.50	$53,098.05	$54,690.99	$56,331.72	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 1000 hours	Optional Subscription License	$66,000.00	$67,980.00	$70,019.40	$72,119.98	$74,283.58	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 5000 hours	Optional Subscription License	$61.00	$62.83	$64.71	$66.65	$68.65	FedRAMP Audio and Video redaction. Hourly rate for volume of 5,000 hours per year

Table 3: Software Licensing & Implementation Fees: Years 6-10

Product / Service	Item & Fee Type	Year 6	Year 7	Year 8	Year 9	Year 10	Comments
ArkCase-USR-FedRAMP (50)	Subscription License	$1,744.47	$1,796.80	$1,850.70	$1,906.22	$1,963.41	Annual cost per user
ArkCase-USR-FedRAMP (51-100)	Subscription License	$1,133.90	$1,167.92	$1,202.96	$1,239.05	$1,276.22	Annual cost per user
ArkCase-USR-FedRAMP (101-200)	Subscription License	$737.05	$759.16	$781.93	$805.39	$829.55	Annual cost per user
ArkCase-USR-FedRAMP (201-300)	Subscription License	$663.34	$683.24	$703.74	$724.85	$746.60	Annual cost per user
ArkCase-USR-FedRAMP (301-500)	Subscription License	$597.00	$614.91	$633.36	$652.36	$671.93	Annual cost per user
ArkCase-USR-FedRAMP (501-1000)	Subscription License	$537.30	$553.42	$570.02	$587.12	$604.73	Annual cost per user
ArkCase-USR-FedRAMP (1001-2000)	Subscription License	$483.57	$498.08	$513.02	$528.41	$544.26	Annual cost per user
ArkCase-USR-FedRAMP (2000 +)	Subscription License	$435.22	$448.28	$461.73	$475.58	$489.85	Annual cost per user
ArkCase-USR-FedRAMP Contributor (50)	Subscription License	$523.34	$539.04	$555.21	$571.87	$589.03	Annual cost per user
ArkCase-USR-FedRAMP Contributor (51-100)	Subscription License	$340.18	$350.39	$360.90	$371.73	$382.88	Annual cost per user
ArkCase-USR-FedRAMP Contributor (101-200)	Subscription License	$221.11	$227.74	$234.57	$241.61	$248.86	Annual cost per user
ArkCase-USR-FedRAMP Contributor (201-300)	Subscription License	$199.00	$204.97	$211.12	$217.45	$223.97	Annual cost per user
ArkCase-USR-FedRAMP Contributor (301-500)	Subscription License	$179.10	$184.47	$190.00	$195.70	$201.57	Annual cost per user
ArkCase-USR-FedRAMP Contributor (501-1000)	Subscription License	$161.21	$166.05	$171.03	$176.16	$181.44	Annual cost per user

ArkCase-USR-FedRAMP Contributor (1001-2000)	Subscription License	$145.07	$149.42	$153.90	$158.52	$163.28	Annual cost per user
ArkCase-USR-FedRAMP Contributor (2000 +)	Subscription License	$130.55	$134.47	$138.50	$142.66	$146.94	Annual cost per user
SOM Enterprise FOIA Platform	One-Time Implementation Fee	$0.00	$0.00	$0.00	$0.00	$0.00	One-time setup of the base Enterprise FOIA Platform
Department Large/Complex (separate deployment)	Onboarding Fee, Per Request	$154,925.84	$159,573.62	$164,360.83	$169,291.65	$174,370.40	Separate deployment based on Enterprise FOIA
Department Medium/Large (minor customizations leveraging SOM Enterprise FOIA)	Onboarding Fee, Per Request	$91,643.85	$94,393.17	$97,224.97	$100,141.72	$103,145.97	Leverage Enterprise FOIA. Custom Portal. Up to 3 custom reports and custom templates.
Department Small (no customizations leveraging SOM Enterprise FOIA)	Onboarding Fee, Per Request	$32,876.14	$33,862.42	$34,878.29	$35,924.64	$37,002.38	Leverage existing portal, workflow, reporting. Adding up to 50 users and groups. 2 virtual training sessions.
Custom Report	One-Time Fee, Per Request	$4,347.28	$4,477.70	$4,612.03	$4,750.39	$4,892.90	Up to 10 columns with lookups and calculations,
Custom Correspondence Template	One-Time Fee, Per Request	$1,738.91	$1,791.08	$1,844.81	$1,900.15	$1,957.15	10 fields or less
Custom Portal	One-Time Fee, Per Request	$9,895.57	$10,192.44	$10,498.21	$10,813.16	$11,137.55	Single page custom portal based on existing external portal
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 100 hours	Optional Subscription License	$12,114.42	$12,477.85	$12,852.19	$13,237.76	$13,634.89	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 250 hours	Optional Subscription License	$28,692.04	$29,552.80	$30,439.38	$31,352.56	$32,293.14	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 400 hours	Optional Subscription License	$38,256.04	$39,403.72	$40,585.83	$41,803.40	$43,057.50	FedRAMP Audio and Video redaction

Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 700 hours	Optional Subscription License	$58,021.67	$59,762.32	$61,555.19	$63,401.85	$65,303.91	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 1000 hours	Optional Subscription License	$76,512.09	$78,807.45	$81,171.67	$83,606.82	$86,115.02	FedRAMP Audio and Video redaction
Veritone Redact - Intelligent Audio, Image and Video Evidence Redaction - 5000 hours	Optional Subscription License	$70.71	$72.83	$75.01	$77.26	$79.58	FedRAMP Audio and Video redaction. Hourly rate for volume of 5,000 hours per year

Note:

- ArkCase-USR-FedRAMP – an Internal user with full access to include document management and redaction capabilities
- ArkCase-USR-FedRAMP Contributor – an Internal user with the ability to add documents /content to support a FOIA request

Table 4: Rate Card for Ancillary Professional Services

Staff Role	Key or Non-Key	Onsite Hourly Rate	Offsite Hourly Rate
Project Manager	Key	$136.39	$143.57
Security Officer	Key	$133.21	$140.22
Business Analyst Lead	Non-Key	$127.30	$134.00
Business Analyst	Non-Key	$109.01	$114.75
Training Lead	Non-Key	$122.04	$128.46
Trainer	Non-Key	$88.83	$93.51
Data Architect	Non-Key	$131.40	$138.32
Lead Developer	Non-Key	$124.69	$131.25
Developer	Non-Key	$108.70	$114.42
Technical Writer	Non-Key	$69.87	$73.55
Other:	Non-Key	$74.24	$78.15
Other:	Non-Key	$129.75	$136.58

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 or authorization, and audited financial statements.

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, if any, carry and maintain insurance coverage as applicable to the subcontracted service(s).

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.
Umbrella or Excess Liability Insurance	
Minimum Limits: **$5,000,000 General Aggregate**	**Contractor must have their policy follow form.**
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.
Crime (Fidelity) Insurance	
Minimum Limits: **$1,000,000 Employee Theft Per Loss**	Contractor must have their policy: (1) cover forgery and alteration, theft of money and securities, robbery and safe burglary, computer fraud, funds transfer fraud, money order and counterfeit currency, and (2) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as Loss Payees.
Professional Liability (Errors and Omissions) Insurance	
Minimum Limits: **$1,000,000 Each Occurrence** **$1,000,000 Annual Aggregate**	

8. **Notice of Non-Compliance.** Contractor consents to receiving electronic communications from a third-party service provider, Origami Risk, for the exclusive purpose of notifying Contractor of non-compliance with the requirements set forth in this Schedule C.
9. **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)

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 is 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 periods 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 Monday – Friday, 8am – 5pm Eastern Time.

“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 Availability 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 99.98% of the time. Availability will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) x 100 = 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 least 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 7:00 p.m. and 10 p.m. Eastern Time on Friday OR 8:00 a.m. to 10:00 p.m. Eastern Time on Saturday adhering to Armedia's standard maintenance operations ; 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 2 seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the calculation of Availability.

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 is 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**
≥99.5%	None
<99.5% but ≥99.0%	10%
<99.0% but ≥95.0%	30%
<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, Support Hours.

(c) provide unlimited online support 24 hours a day, seven days a week;

(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 During Normal Business Hours

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. If the Contractor Resolves the Support Request by way of a work-around accepted in writing by the State, the support classification assessment will be reduced to a High Service Error.
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 5 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 at no additional cost.

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 24 hours, and a Recovery Time Objective (RTO) of 8 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.

7. Hardware – RESERVED.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

First Person	Alexander Schaaf | ARMEDIA Help Desk Tier I e. support@arkcase.com or chat: http://www.arkcase.com e. alexander.schaaf@armedia.com a. 8221 Old Courthouse Rd Suite 300, Vienna, VA 22181, USA
Second Person	Sanija Shabani | ARMEDIA Project Manager m. (770) 601-6888 | e. sanija.shabani@armedia.com a. 8221 Old Courthouse Rd Suite 300, Vienna, VA 22181, USA
Third Person	John Shinnick | ARMEDIA CTO **p.** (571) 395-4800 | **m.** (678) 596-7775 | **e.** jshinnick@armedia.com a. 8221 Old Courthouse Rd Suite 300, Vienna, VA 22181, USA

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, and backed up in the United States or its territories. The use of Offshore Resources is not permitted;

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 programing 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 E, ATTACHMENT 1 – PCI COMPLIANCE & CEPAS

1. PCI Compliance.

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

The Contractor must notify the State's Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, Discover, and American Express) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.

Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must 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 breach.

The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

The Contractor must provide the State's Contract Administrator with an annual Attestation of Compliance (AOC) if or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

2. CEPAS Electronic Receipt Processing Standard.

All electronic commerce applications that allow for electronic receipt of credit or debit card and electronic check transactions must be processed via the State's Centralized Electronic Payment Authorization System (CEPAS). To minimize the risk to the State, full credit/debit card numbers,

sensitive authentication data, and full bank account information must never be stored on state-owned IT resources. For additional information, refer to the CEPAS Integration Guide that can be found at, once bidder signs an NDA:

https://stateofmichigan.sharepoint.com/teams/insidetreasury/about-treasury/work-areas/Documents/CEPAS/Integration%20Guides%20and%20Hotfix%20Notes/PayPoint%20Merchant%20Integration%20Guide%202.14.2021.pdf?CT=1623169629598&OR=Outlook-Body&CID=97F008F1-D094-4ED7-9335-63E0B12988E6

SCHEDULE E, ATTACHMENT 2 – CJIS

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI 1000

Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

SCHEDULE E, ATTACHMENT 3 – FERPA

Contractor must comply with the Family Educational Rights and Privacy Act (FERPA), and any related rules and regulations, including but not limited to 34 C.F.R. Part 99. In addition, Contractor must obligate its Permitted Subcontractor(s), in writing, to the requirements of Schedule E - Data Security Requirements, including this Attachment.

SCHEDULE E, ATTACHMENT 4 – HIPAA BUSINESS ASSOCIATE ADDENDUM

HIPAA BUSINESS ASSOCIATE AGREEMENT

The parties to this Business Associate Agreement ("Agreement") are the Michigan Department of Technology, Management and Budget ("DTMB", "Business Associate 1") on behalf of Michigan Department of Health and Human Services (MDHHS) ("Covered Entity") and Armedia, LLC "Business Associate 2".

RECITALS

A. Under this Agreement, Business Associate 2 will collect or receive certain information on the Covered Entity's behalf, some of which may constitute Protected Health Information ("PHI"). In consideration of the receipt of PHI, the Business Associate agrees to protect the privacy and security of the information as set forth in this Agreement.

B. Covered Entity and each Business Associate intend to protect the privacy and provide for the security of PHI collected or received by the Business Associate under the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and the HIPAA Rules, as amended.

C. The HIPAA Rules require the Covered Entity to enter into an agreement containing specific requirements with Business Associate 1, and likewise Business Associate 1 must enter an agreement with Business Associate 2 before the Business Associate 2's receipt of PHI.

AGREEMENT

1. Definitions.

a. The following terms used in this Agreement have the same meaning as those terms in the HIPAA Rules: Breach; Data Aggregation; Designated Record Set; Disclosure; Health Care Obligations; Individual; Minimum Necessary; Notice of Privacy Practices; Protected Health Information; Required by Law; Secretary; Security Incident; Security Measures, Subcontractor; Unsecured Protected Health Information, and Use.

b. "Business Associate" has the same meaning as the term "business associate" at 45 CFR 160.103 and regarding this Agreement means DTMB ("Business Associate 1") and **[Contractor]** ("Business Associate 2").

c. "Covered Entity" has the same meaning as the term "covered entity" at 45 CFR 160.103 and regarding this Agreement means MDHHS.

d. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Obligations of Business Associate 2.

Business Associate 2 agrees to:

a. use and disclose PHI only as permitted or required by this Agreement or as required by law.

b. implement and use appropriate safeguards and comply with Subpart C of 45 CFR 164 regarding electronic protected health information, to prevent use or disclosure of PHI other than as provided in this Agreement. Business Associate 2 must maintain, and provide a copy to the Covered Entity and Business Associate 1 within 10 days of a request from the Covered Entity or Business Associate 1, a comprehensive written information privacy and security program that includes security measures that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI relative to the size and complexity of Business Associate 2's operations and the nature and the scope of its activities.

c. report to the Covered Entity and Business Associate 1 within 24 hours of any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of Unsecured Protected Health Information as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. If Business Associate 2 is responsible for any unauthorized use or disclosure of PHI, it must promptly act as required by applicable federal and State laws and regulations. Covered Entity and Business Associate 2 will cooperate in investigating whether a breach has occurred, to decide how to provide breach notifications to individuals, the federal Health and Human Services' Office for Civil Rights, and potentially the media.

d. ensure, according to 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate 2 agree to the same restrictions, conditions, and requirements that apply to Business Associate 2 regarding such information. Each subcontractor must sign an agreement with Business Associate 2 containing substantially the same provisions as this Agreement and further identifying Business Associate 1 and Covered Entity as a third-party beneficiary of the agreement with the subcontractor. Business Associate 2 must implement and maintain sanctions against subcontractors that violate such restrictions and conditions and must mitigate the effects of any such violation.

e. make available PHI in a Designated Record Set to the Covered Entity within 10 days of a request from the Covered Entity to satisfy the Covered Entity's obligations under 45 CFR 164.524.

f. within ten days of a request from the Covered Entity, amend PHI in a Designated Record Set under, 45 CFR § 164.526. If any individual requests an amendment of PHI directly from Business Associate 2 or its agents or subcontractors, Business Associate 2 must notify the Covered Entity in writing within five days of the request and amend the information within ten days of the request. Any denial of amendment of PHI maintained by Business Associate 2 or its agents or subcontractors is the responsibility of Business Associate 2.

g. maintain, and within ten days of a request from the Covered Entity make available, the information required to provide an accounting of disclosures to enable the Covered Entity to fulfill its obligations under 45 CFR § 164.528. Business Associate 2 is not required to provide an accounting to the Covered Entity of disclosures: (i) to carry out treatment, payment or health care operations, as set forth in 45 CFR § 164.506; (ii) to individuals of PHI about them as set forth in 45 CFR § 164.502; (iii) under an authorization as provided in 45 CFR § 164.508; (iv) to persons involved in the individual's care or other notification purposes as set forth in 45 CFR § 164.510; (v) for national security or intelligence purposes as set forth in 45 CFR § 164.512(k)(2); (vi) to correctional institutions or law enforcement officials as set forth in 45 CFR § 164.512(k)(5); (vii) as part of a limited data set according to 45 CFR 164.514(e); or (viii) that occurred before the compliance date for the Covered Entity. Business Associate 2 agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate 2 and its agents or subcontractors for at least six years before the request, but not before the compliance date of the Privacy Rule. At a minimum, such information must include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure. If the request for an accounting is delivered directly to Business Associate 2 or its agents or subcontractors, Business Associate 2 must, within ten days of the receipt of the request, forward it to the Covered Entity in writing.

h. to the extent Business Associate 2 is to carry out one or more of the Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity when performing those obligations.

i. make its internal practices, books, and records relating to Business Associate 2's use and disclosure of PHI available to the Secretary for purposes of determining compliance with the HIPAA Rules. Business Associate 2 must concurrently provide to the Covered Entity a copy of any PHI that the Business Associate 2 provides to the Secretary.

j. retain all PHI throughout the term of the Agreement and for a period of six years from the date of creation or the date when it last was in effect, whichever is later, or as required by law. This obligation survives the termination of the Agreement.

k. implement policies and procedures for the final disposition of PHI and the hardware and equipment on which it is stored, including but not limited to, removal of PHI before re-use.

l. within ten days of a written request by the Covered Entity, Business Associate 2 and its agents or subcontractors must allow the Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI under this Agreement. Business Associate 2 and the Covered Entity will mutually agree in advance upon the scope, timing and location of such an inspection. Covered Entity must protect the confidentiality of all confidential and proprietary information of Business Associate 2 to which the Covered Entity has access during the course of such inspection. Covered Entity and Business Associate 2 will execute a nondisclosure agreement, if requested by the other party. The fact that the Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate 2's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate 2 of its responsibility to comply with this Agreement. Covered Entity's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, does not constitute acceptance of such practice or a waiver of the Covered Entity's enforcement rights under this Agreement.

3. Permitted Uses and Disclosures by the Business Associate.

a. Business Associate 2 may use or disclose PHI:

(1) for the proper management and administration of Business Associate 2 or to carry out the legal responsibilities of Business Associate 2; provided, however, either (A) the disclosures are required by law, or (B) Business Associate 2 obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate 2 of any instances of which it is aware in which the confidentiality of the information has been breached;

(2) as required by law;

(3) for Data Aggregation services relating to the health care operations of the Covered Entity;

(4) to de-identify, consistent with 45 CFR 164.514(a) – (c), PHI it receives from the Covered Entity. If Business Associates 2 de-identifies the PHI it receives from the Covered Entity,

Business Associate 2 may use the de-identified information for any purpose not prohibited by the HIPAA Rules; and

(5) for any other purpose listed here: management of the Solution.

b. Business Associate 2 agrees to make uses and disclosures and requests for PHI consistent with the Covered Entity's minimum necessary policies and procedures.

c. Business Associate 2 may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Covered Entity except for the specific uses and disclosures described above in 3(a)(i) and (iii).

4. Covered Entity's Obligations

Covered entity agrees to:

a. use its Security Measures to reasonably and appropriately maintain and ensure the confidentiality, integrity, and availability of PHI transmitted to Business Associate 2 under this Agreement until the PHI is received by Business Associate 2.

b. provide Business Associate 2 with a copy of its Notice of Privacy Practices and must notify the Business Associate of any limitations in the Notice of Privacy Practices of the Covered Entity under 45 CFR 164.520 to the extent that such limitation may affect Business Associate 2's use or disclosure of PHI.

c. notify Business Associate 2 of any changes in, or revocation of, the permission by an individual to use or disclose the individual's PHI to the extent that such changes may affect Business Associate 2's use or disclosure of PHI.

d. notify Business Associate 2 of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522 to the extent that such restriction may affect Business Associate 2's use or disclosure of PHI.

5. Term. This Agreement continues in effect until terminated or is replaced with a new agreement between the parties containing provisions meeting the requirements of the HIPAA Rules, whichever first occurs.

6. Termination.

a. Material Breach. In addition to any other provisions in the Agreement regarding breach, a breach by Business Associate 2 of any provision of this Agreement, as determined by the Covered Entity, constitutes a material breach of the Agreement and provides grounds for Business Associate 1 to terminate this Agreement for cause at the request of Covered Entity. Termination for cause is subject to 6.b.:

(1) Default. If Business Associate 2 refuses or fails to timely perform any of the provisions of this Agreement, the Covered Entity may notify Business Associate 2 in writing of the non-performance, and if not corrected within thirty days, Business Associate 1 may immediately terminate the Agreement at the request of Covered Entity. The Business Associate 2 must continue performance of the Agreement to the extent it is not terminated.

(2) Business Associate 2's Duties. Notwithstanding termination of the Agreement, and subject to any directions from the Covered Entity or Business Associate 1, Business Associate 2 must protect and preserve property in the possession of Business Associate 2 in which the Covered Entity has an interest.

(3) Erroneous Termination for Default. If Business Associate 1 terminates this Agreement at the request of Covered Entity under Section 6(a) and after such termination it is determined, for any reason, that Business Associate 2 was not in default, then such termination will be treated as a termination for convenience, and the rights and obligations of the parties will be the same as if the Agreement had been terminated for convenience.

b. Reasonable Steps to Cure Breach. If the Covered Entity or Business Associate 1 knows of a pattern of activity or practice of Business Associate 2 that constitutes a material breach or violation of Business Associate 2's obligations under the provisions of this Agreement or another arrangement and does not terminate this Agreement under Section 6(a), then the Business Associate 1, at the request of Covered Entity or on its own accord, must notify Business Associate 2 of the pattern of activity or practice. Business Associate 2 must then take reasonable steps to cure such breach or end such violation, as applicable. If the Business Associate 2's efforts to cure such breach or end such violation are unsuccessful, Business Associate 1, at the request of the Covered Entity or on its own accord, may either (i) terminate this Agreement, if feasible or (ii) report Business Associate 2's breach or violation to the Secretary.

c. Effect of Termination. After termination of this Agreement for any reason, the Business Associate, with respect to PHI it received from the Covered Entity, or created, maintained, or received by Business Associate 2 on behalf of the Covered Entity, must:

(1) retain only that PHI which is necessary for Business Associate 2 to continue its proper management and administration or to carry out its legal responsibilities;

(2) return to the Covered Entity (or, if agreed to by the Covered Entity in writing, destroy) the remaining PHI that Business Associate 2 still maintains in any form;

(3) continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate 2 retains the PHI;

(4) not use or disclose the PHI retained by Business Associate 2 other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section 3(a)(1) which applied before termination; and

(5) return to the Covered Entity (or, if agreed to by the Covered Entity in writing, destroy) the PHI retained by Business Associate 2 when it is no longer needed by Business Associate 2 for its proper management and administration or to carry out its legal responsibilities.

7. No Waiver of Immunity. The parties do not intend to waive any of the immunities, rights, benefits, protection, or other provisions of the Michigan Governmental Immunity Act, MCL 691.1401, *et seq*., the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq.*, or the common law.

8. Data Ownership. Business Associate 2 has no ownership rights in the PHI. The covered entity retains all ownership rights of the PHI.

9. Disclaimer. Neither Business Associate 1, nor the Covered Entity, warrants or represents that compliance by Business Associate 2 with this Agreement, HIPAA, or the HIPAA Rules will be adequate or satisfactory for Business Associate 2's own purposes. Business Associate 2 is solely responsible for all decisions made by Business Associate 2 regarding the safeguarding of PHI.

10. Certification. If the Covered Entity determines an examination is necessary to comply with the Covered Entity's legal obligations under HIPAA relating to certification of its security practices, the Covered Entity or its authorized agents or contractors, may, at the Covered Entity's expense, examine Business Associate 2's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to the Covered Entity the extent to which Business Associate 2's security safeguards comply with HIPAA, the HIPAA Rules or this Agreement.

11. Amendment. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA and the HIPAA Rules. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of HIPAA and the HIPAA Rules. Either party may terminate the Agreement upon thirty days written notice if (i) one party does not promptly enter into negotiations to amend this Agreement when requested by the other party or (ii) Business Associate 2 does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that the Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA or the HIPAA Rules.

12. Assistance in Litigation or Administrative Proceedings. Business Associate 2 must make itself, and any subcontractors, employees or agents assisting Business Associate 2 in the

performance of its obligations under this Agreement, available to the Covered Entity or Business Associate 1, at no cost to the Covered Entity or Business Associate 1, to testify as witnesses, or otherwise, if litigation or administrative proceedings are commenced against the Covered Entity or Business Associate 1, its directors, officers or employees, departments, agencies, or divisions based upon a claimed violation of HIPAA or the HIPAA Rules or other laws relating to Business Associate 2's or its subcontractors use or disclosure of PHI under this Agreement, except where Business Associate 2 or its subcontractor, employee or agent is a named adverse party.

13. No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer upon any person other than the Covered Entity, Business Associate 1, Business Associate 2 and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

14. Interpretation and Order of Precedence. Any ambiguity in this Agreement must be interpreted to permit compliance with the HIPAA Rules. Where the provisions of this Agreement differ from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Agreement control.

15. Effective Date. This Agreement is effective upon receipt of the last approval necessary and the affixing of the last signature required.

16. Survival of Certain Agreement Terms. Notwithstanding any contrary provision in this Agreement, the Business Associate 2's obligations under Section 6(d) and record retention laws ("Effect of Termination") and Section 12 ("No Third-Party Beneficiaries") survive termination of this Agreement and are enforceable by the Covered Entity or Business Associate 1.

17. Representatives and Notice.

a. Representatives. The individuals listed below are designated as the parties' respective representatives for purposes of this Agreement. Either party may from time to time designate in writing new or substitute representatives.

b. Notices. All required notices must be in writing and must be hand delivered or given by certified or registered mail to the representatives at the addresses set forth below.

Covered Entity Representative

James Bowen
Security and Data Governance Director
MDHHS Compliance Office
235 South Grand Ave, 4th Floor
Lansing, MI 48933
(517) 284-1018
MDHHSPrivacySecurity@michigan.gov

Business Associate 1 Representative:

Name: Duane
Title:
Department:
Address:
Phone:
Email:

Business Associate 2 Representative: **[Contractor]**

Name:
Title:
Department:
Address:
Phone:
Email:

Any notice given to a party under this Agreement shall be deemed effective, if addressed to such party, upon: (i) delivery, if hand delivered; or (ii) the third Business Day after being sent by certified or registered mail.

DTMB as Business Associate 1, on behalf of MDHHS	**Business Associate 2**
	[INSERT NAME]
By: _____	By: _____
Date: _____	Date: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____

SCHEDULE E, ATTACHMENT 5 – IRS PUBLICATION 1075 EXHIBIT 7

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

SCHEDULE E, ATTACHMENT 6 – MICHIGAN TREASURY ATTACHMENT B: SAFEGUARD REQUIREMENTS OF CONFIDENTIAL TAX DATA

This section sets forth the safeguard requirements for handling, storage, and processing of confidential tax information for a Contractor and their subcontractor(s) and is incorporated as an integral part of the Contract. It will facilitate administration and enforcement of the laws of the State of Michigan in a manner consistent with the applicable statutes, regulations, published rules and procedures or written communication.

I. Authority

Authority for the Michigan Department of Treasury to require that this section be included in the Contract is contained in l941 PA 122, as amended, MCL 205.28(1)(f), which subjects current or former contractors to the same restrictions and penalties imposed upon department employees regarding the treatment of confidential information. A private contractor or its employees are strictly prohibited from disclosing taxpayer information to a third party. The prohibition against disclosure does not bar an employee of a private contractor with whom the State of Michigan (State) contracts that processes tax returns or payments pursuant to the Contract from having access to confidential information that is reasonably required for the processing or collection of amounts due this State. Private contractors and any subcontractors will follow Treasury guidelines for Authorized representatives.

II. Confidentiality

It is agreed that all information exchanged under this section will be kept confidential in accordance with the confidentiality provisions contained in the Revenue Act, MCL 205.28(1)(f)-which states in part;

> "Except as otherwise provided in this subdivision, an employee, authorized representative, or former employee or authorized representative of the department or anyone connected with the department will not divulge any facts or information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the department for a tax administered by the department."

Confidential information obtained under this contract will not be disclosed except as required by state law, or in the proper administration of applicable laws, promulgated rules and procedures. In the event, confidentiality statutes are amended, Treasury will notify Contractor of any changes. No employee, agent, authorized representative or legal representative of Contractor will disclose any information obtained by virtue of this section to any other division within their company or any other governmental agency, department or unit within such governmental agency whether local, state, federal or foreign, department or unit within such governmental agency, or any unauthorized third

party. No tax returns or tax return information accessed by Contractor will be duplicated or disseminated within or outside the company without the written approval of the Contract Compliance Inspector. Tax returns and tax return information remain the property of Treasury.

Contractor may use a taxpayer's name, address and Social Security number or employer identification number to the extent necessary in connection with the processing and mailing of forms for any report or return required in the administration of any tax in the performance of the Contract. The use of the Social Security number must be in accordance with the state Social Security Number Privacy Act 454 of 2004, as amended.

Confidential information obtained under this agreement will not be disclosed in part of a report or document that is subject to FOIA.

The penalties for violating the confidentiality provisions of the Revenue Act are contained in, MCL 205.28(2) and MCL 205.27(4). MCL 205.28(2) states:

> "A person who violates subsection (1)(e), (1)(f), (4) or (5) is guilty of a felony, punishable by a fine of not more than $5,000.00, or imprisonment for not more than 5 years, or both, together with the costs of prosecution. In addition, if the offense is committed by an employee of this state, the person will be dismissed from office or discharged from employment upon conviction."

MCL 205.27(4) states:

> A person who is not in violation pursuant to subsection (2), but who knowingly violates any other provision of this act, or of any statute administered under this act, is guilty of a misdemeanor, punishable by a fine of not more than $1,000.00, or imprisonment for not more than 1 year, or both.

Information received by Treasury from the U.S. Internal Revenue Service, pursuant to section 6103(d) of the Internal Revenue Code or any other federal agency will not be subject to the exchange.

III. Procedure for Security

Contractor will safeguard any tax return information obtained under the Contract as follows:

A. Access to the tax returns and tax return information will be allowed only to those authorized employees and officials of Contractor who need the information to perform their official duties in connection with the uses of the information authorized in this Contract.

B. Any records created from tax returns and tax return information will be stored in an area that is physically safe from access by unauthorized persons during duty hours and locked in a secure area during non-duty hours, or when not in use.

C. Any records matched and any records created by the match will be processed under the immediate supervision and control of authorized personnel in a manner in which will protect the confidentiality

of the records, and in such a way that unauthorized persons cannot retrieve any such records by means of a computer, remote terminal or other means.

D. All personnel who will have access to the tax returns and tax return information and to any records created by the tax return information will be advised annually of the confidential nature of the information, the safeguards required to protect the information and the civil and criminal sanctions for noncompliance contained in MCL 205.28 (2) and MCL 205.27(4) and will sign confidentiality certifications.

E. All confidential information, electronic and paper, will be secured from unauthorized access and with access limited to designated personnel only. State tax return information will not be commingled with other information. All Michigan tax returns and return information will be marked as follows: **CONFIDENTIAL - DO NOT DISCLOSE - MICHIGAN TREASURY TAX RETURN INFORMATION**

F. Treasury, Office of Privacy and Security or Contract Compliance Inspector may make onsite inspections or make other provisions to ensure that adequate safeguards are being maintained by the Contractor.

G. The Treasury Office of Privacy and Security may monitor compliance of systems security requirements during the lifetime of the Contract or any extension.

H. Contractor will also adopt policies and procedures to ensure that information contained in their respective records and obtained from Treasury and taxpayers will be used solely as stipulated in the Contract.

IV. Computer System Security of Tax Data

The identification of confidential tax records and defining security controls are intended to protect Treasury tax return information from unlawful disclosure, modification, destruction of information and unauthorized secondary uses.

Computer system security and physical security of tax data stored and processed by Contractor must be in compliance with the following security guidelines and standards established by Treasury. These guidelines apply to any computer system developed by Contractor, either through its own systems staff, or through a contractor, subcontractor or vendor):

A. Controlled Access Protection

All computer systems processing, storing and transmitting Michigan tax information must have computer access protection controls These security standards are delineated in the National Institute of Standards and Technology (NIST) Special Publications number 800-53 "Recommended Security Controls for the Federal Information Systems" at http://csrc.nist.gov/publications/PubsSPs.html. To meet these standards, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance, and documentation.

1) **Security Policy** – A security policy is a written document describing the system in terms of categories of data processed, users allowed access and access rules between the users and the data. Additionally, it describes procedures to prevent unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of or into the system. Further protection must be provided where the computer system contains information for more than one program/project, office, or Agency and that personnel do not have authorization to see all information on the system.

2) **Accountability** – Computer systems processing Michigan tax information must be secured from unauthorized access. All security features must be available (audit trails, identification and authentication) and activated to prevent unauthorized users from indiscriminately accessing Michigan tax information. Everyone who accesses computer systems containing Michigan tax information is accountable. Access controls must be maintained to ensure that unauthorized access does not go undetected. Computer programmers and contractors who have a need to access databases, and are authorized under the law, must be held accountable for the work performed on the system. The use of passwords and access control measures must be in place to identify who accessed protected information and limit that access to persons with a need to know.

   a) On-line Access –Users will be limited to any Treasury on-line functions, by limiting access through functional processing controls and organization restrictions.

   Any employee granted access privileges through the Contractor's Security Administrator will be approved for access and viewing rights to Treasury on-line systems by the Department of Treasury, Office of Privacy and Security.

   b) Operating Features of System Security
   Contractor must meet the following levels of protection with respect to tax return information. Individual user accountability must be ensured through user identification number and password.

   i. Access rights to confidential tax information must be secured through appropriate levels of authorization.

   ii. An audit trail must be maintained of accesses made to confidential information.

   iii. All confidential and protected information must be cleared from a system before it is used for other purposes not related to the enforcement, collection or exchange of data not covered by this section or by an addendum to this Contract.

   iv. Hard copies made of confidential tax return information must be labeled as confidential information.

   v. Confidential Treasury tax information will be blocked or coded as confidential on system.

vi. Any computer system in which Michigan tax return information resides must systematically notify all users upon log-in of the following disclosure penalties for improperly accessing or making an authorized disclosure of Michigan tax return information:

NOTICE TO EMPLOYEES AND AUTHORIZED REPRESENTATIVES

This system contains Michigan Department of Treasury tax return information. **DO NOT DISCLOSE OR DISCUSS MICHIGAN RELATED TAX RETURN INFORMATION** with unauthorized individuals. The Revenue Act at MCL 205.28(1)(f) prohibits such disclosure.

MICHIGAN PENALTIES
A person making a willful unauthorized disclosure or inspection (browsing) of tax return information may be charged with the following Michigan penalties:

- Criminal penalties up to $5,000 and/or imprisonment for 5 years, plus costs and dismissal from employment if it is found that a current or former employee or authorized representative has made an unauthorized disclosure of a tax return or tax return information or divulged audit selection or processing parameters. [MCL 205.28(2)]

- A misdemeanor, punishable by a fine of not more than $1,000.00, or imprisonment for not more than 1 year, or both if the person is not in violation pursuant to MCL 205.27(2), but who knowingly violates any other provision of this act, or of any statute administered under this act.

This statement is subject to modification. A confidentiality statement, subject to modification, will be sent as needed by the Security Administrator to all employees, contractors, and legal representatives of Contractor.

3) **Assurance** – Contractor must ensure that all access controls and other security features are implemented and are working when installed on their computer system. Significant enhancements or other changes to a security system must follow the process of review, independent testing, and installation assurance. The security system must be tested at least annually to assure it is functioning correctly. All anomalies must be corrected immediately.

a) The Contractor must initiate corrective action for all non-conformities as soon as detected and immediately advise the Contract Compliance Inspector. Notice of the corrective action must be provided to the Contract Compliance Inspector. All non-conformities must be reported to the Contract Compliance Inspector with the following:

a. Duration of non-conformity/interruption
b. Reason for non-conformity/interruption
c. Resolution.

b) All non-conformities to the specifications/tasks of the Contract must be corrected

within four (4) hours. The State recognizes there will be instances when adherence to this time frame will not be possible. However, the State will only tolerate this on an exception basis. To request an exception to this time frame, the Contractor must submit a detailed project plan to address the non-conformity within four (4) hours to the Contract Compliance Inspector for approval.

4) **Documentation** – Design and test documentation must be readily available to the state. The developer or manufacturer should initially explain the security mechanisms, how they are implemented and their adequacy (limitations). This information should be passed on to the security officer or supervisor. Test documentation should describe how and what mechanisms were tested and the results. If recognized organizations/tests/standards are used, then a document to that effect will suffice. For example, a system that has been tested and certified as meeting certain criteria may have a document stating this fact, without detailed tests/results of information. Contractor, however, must ensure the documentation covers the exact system and that it includes the specific computer system used by Contractor.

   Additionally, documentation must include a security administrator's guide. The security administrator's guide is addressed to the System's Administrator and Security Officer and will describe the protection mechanisms provided by the security system, guidelines on their use and how they interact. This document will present cautions about security functions and describe privileges that should be controlled when running a secure system. The document will be secured and locked at all times with access rights only by the Systems Administrator and Security Officer.

Note: When a security system is designed or purchased for a specific computer or computer system, the security mechanisms must be reviewed by the State to ensure that needed security parameters are met. An independent test should be implemented on the specific computer or computer system to ensure that the security system meets the security parameters within this contract and developed with the computer system. The test may be arranged by the developer but must be done by an independent organization. Contractor must assign responsible individuals (Security Officers) with knowledge of information technology and applications to oversee the testing process. These individuals must be familiar with technical controls used to protect the system from unauthorized entry.

Finally, contingency and backup plans must be in place to ensure protection of Michigan tax information.

V. Electronic Transmission of Michigan Tax Information

The two acceptable methods of transmitting Michigan tax information over telecommunications devices are encryption and using guided media. Encryption involves altering data objects in a way that the objects become unreadable until deciphered with the appropriate software at the intended destination. Guided media involves transmission of data over twisted pair cable, coaxial cable or end to end fiber optics which are typically used in secure computer networks like the state's Local Area Network (LAN), telephone systems, and television distribution.

Cryptography standards have been adopted by the IRS and can be used to provide guidance for encryption, message authentication codes or digital signatures and digital signatures with or without an associated certification infrastructure. For further information, see IRS Publication 1075 at the IRS web site.

Unencrypted cable circuits of fiber optics are an acceptable alternative for transmitting Michigan tax information. Adequate measures must be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio or microwave transmission. Additional precautions should be taken to protect the cable, i.e., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms and switching centers.

A. **Remote Access**

Accessing databases containing Michigan tax information from a remote location – that is, a location not directly connected to the Local Area Network (LAN) will require adequate safeguards to prevent unauthorized entry.

For remote access, the contractor is required to use an identification security card that requires both PIN and card in possession. The State identified and approved methods for remote vendor access are as follows:

- SecureID through VPN – State provided SecureID taken and VPN software in order to access State of Michigan resources. Appropriate Acceptable Use policies and signoffs are required
- Follow-the Sun SecureID – Vendor is provided with VPN software and a State of Michigan technical resource coordinates with the DTMB Client Service Center to provide secure ID code access to specific State of Michigan resources. Appropriate Acceptable Use Policies and signoffs are required.

B. **Portable Computer Devices**

Any entrusted confidential information collected or accessed during this Contract must be encrypted when stored on all storage devices and media. This includes, but not limited to, disk drives for servers and workstations, and portable memory media (PDAs, RAM drives, memory sticks, etc.).

VI. Record Keeping Requirements for Information Received

Each Contractor, requesting and receiving information will keep an accurate accounting of the information received. The audit trail will be required which will include the following information:

a. Taxpayer's name
b. Identification number
c. Information requested
d. Purpose of disclosure request
e. Date information received
f. Name of Division and employee making request
g. Name of other employees who may have had access
h. Date destroyed
i. Method of destruction

The Contractor will adopt and implement formal procedures to:

- Ensure proper handling of tax returns and tax return information;
- Secure and safeguard information from unauthorized use; and
- Ensure appropriate destruction of information and materials retrieved from Treasury.

A. Electronic Media

Contractor will keep an inventory of magnetic and electronic media received under the Contract.

Contractor must ensure that the removal of tapes and disks and paper documents containing Michigan tax return information from any storage area is properly recorded on charge-out records. Contractor is accountable for missing tapes, disks, and paper documents.

B. Recordkeeping Requirements of Disclosure Made to State Auditors

When disclosures are made by Contractor to State Auditors, these requirements pertain only in instances where the Auditor General's staff extracts Michigan tax returns or tax information for further review and inclusion in their work papers. Contractor must identify the hard copies of tax records or if the tax information is provided by magnetic tape format or through other electronic means, the identification will contain the approximate number of taxpayer's records, the date of inspection, the best possible description of the records and the name of the Auditor(s) making the inspection.

The Disclosure Officer must be notified, in writing, of any audits done by auditors, internal or otherwise, of Contractor that would involve review of Treasury processing parameters.

VII. Contract Services

To the extent the Contractor employs an independent agency, consultant, or agent to process confidential information which includes Michigan tax return information; the Contractor will notify the Treasury Disclosure Officer before the execution of any such agreement. Each agreement will include in the agreement the following recommended safeguard provisions:

A. The identification of confidential tax records and defining security controls are intended to protect Treasury tax return information from unlawful disclosure, modification, destruction of information and unauthorized secondary uses.

Definition of Treasury Tax Return Information as defined in Revenue Administrative Bulletin (RAB) 1989-39:

> Taxpayer's identity, address, the source or amount of his/her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments whether the taxpayer's return was, is being or will be examined or subject to their investigation or processing, or any other data, received by, recorded by, prepared by, furnished to or collected by the agency with respect to a return or with respect to the determination of the existence, or liability (or the amount thereof) of any person under the tax laws administered by the Department, or related statutes of the state for any tax, penalty, interest, fine, forfeiture, or other imposition or offense. The term "tax return information" also includes any and all account numbers assigned for identification purposes.

B. An acknowledgment that a taxpayer has filed a return is known as a "fact of filing" and may not be disclosed. All tax return data made available in any format will be used only for the purpose of carrying out the provisions of the Contract between Contractor and the sub-contractor. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract between Contractor and the subcontractor. In addition, all related output will be given the same level of protection as required for the source material.

C. The subcontractor will certify that the data processed during the performance of the Contract between Contractor and the subcontractor will be completely purged from all data storage components of the subcontractor's computer facility, and no output will be retained by the subcontractor at the time the work is completed.

D. Destruction of tax data, including any spoilage or any intermediate hard copy printout which may result during the processing of Michigan tax return information, will be documented with a statement containing the date of destruction, description of material destroyed, and the method used. Destruction parameters must meet the standards of Section IX, Disposal of Tax Information, of this agreement.

E. Computer system security and physical security of tax data stored and processed by the subcontractor must be in compliance with security guidelines and standards established by this contract. See section VI (Record Keeping Requirements for Information Received in Paper Format) for more details.

F. The Contractor will be responsible for maintaining a list of employees authorized to access Michigan tax return information and will provide a copy of such list to Treasury.

G. No work involving information furnished under the contract will be subcontracted without the specific approval of Treasury. Contractor and approved subcontractors handling Michigan tax return information will be required to sign the *Vendor, Contractor or Subcontractor Confidentiality Agreement* provided by Treasury, (Form 3337, see Attachment A). The original agreements will be returned to the Disclosure Officer for the Department of Treasury and a copy sent to the Contract Compliance Inspector.

VIII. Transport of Tax Information

In the event, it is necessary to transport confidential tax return information the Contractor is responsible for holding the carrier responsible for safeguarding the records. The Contractor must obtain a signed *Vendor, Contractor or Subcontractor Confidentiality Agreement* (Form 3337, see Attachment A) for each carrier employee who has access to Michigan tax return information. The original agreements will be returned to the Department of Treasury, Disclosure Officer and a copy sent to the Contract Compliance Inspector.

If it is necessary to transfer records and responsibility for transport to a third carrier due to a mishap during transportation, the Contractor is responsible for ensuring safeguard standards remain enforce. This type of incident will be documented in accordance with the incident reporting guidelines in procedure PT-03253, "Incident Reporting and Handling".

Any such incidents must be reported to the Contract Administrator immediately.

IX. Disposal of Tax Information

Materials furnished to Contractor, such as tax returns, remittance vouchers, W-2 reports, correspondence, computer printouts, carbon paper, notes, memorandums and work papers will be destroyed by burning, mulching, pulverizing or shredding. If shredded, destroy paper using cross cut shredders which produce particles that are 1 mm x 5mm (0.04in x 0.2 in.) in size (or smaller).

Data tracks should be overwritten or reformatted a minimum of three times or running a magnetic strip over entire area of disk at least three (3) times to remove or destroy data on the disk media Electronic data residing on any computer systems must be purged based on Treasury's retention schedule.

Contractor and its subcontractor(s) will retain all confidential tax information received by Treasury only for the period of time required for any processing relating to the official duties and then will destroy the records. Any confidential tax information that must be kept to meet evidentiary requirements must be kept in a secured, locked area and properly labeled as confidential return information. See Procedure for Security (Section III of this agreement) for more details.

X. Security Responsibility

Contractor will designate a security person who will ensure that each individual having access to confidential tax information or to any system which processes Michigan tax return information is appropriately screened, trained and executes a *Vendor, Contractor or Subcontractor Confidentiality Agreement* (Form 3337, see Attachment A) before gaining access or transaction rights to any process and computer system containing Treasury tax return information.

Each Contractor or their subcontractor(s) employees' access and transaction rights will be reviewed periodically to ensure that there is a need to know Treasury tax return information displayed in any media.

Michigan tax return information will be made available only to individuals authorized by the Contract. Contractor will maintain a list of persons authorized to request and receive information and will update the list as necessary**.** A copy of the list must be furnished to the Michigan Department of Treasury Disclosure Officer and Contract Compliance Inspector.

XI. Security Breach Notification

The Contractor is required to report to Treasury, on Form 4000, Incident Reporting (Attachment B) any use or disclosure of confidential information, whether suspected or actual, **immediately** after becoming aware of the misuse or disclosure. The Contractor may substitute its internal form for Form 4000 if all pertinent information is included.

The Contractor agrees to immediately contain the breach if it is determined ongoing.

Treasury has the right to terminate the Contract when a breach has occurred, and the Contractor cannot demonstrate proper safeguards were in place to avert a breach. Treasury must approve Contractor's resolution to the breach.

XIII. Certification of Compliance

The Contractor will fully protect State Tax Information (STI) entrusted to them. Each Contractor or subcontractor who will have access to STI must read and sign a confidentiality agreement. This contract requires that all information obtained from the Michigan Department of Treasury under the Revenue Act, PA 122 of 1941, MCL 205.28 (1)(f) be kept confidential. In the event of a security breach involving STI in the possession of the Contractor, the Contractor agrees to provide full cooperation to conduct a thorough security review. The review will validate compliancy with the Contract, and state laws and regulations.

If, as a result of the Contractor's failure to perform as agreed, the State is challenged by a governmental authority or third party as to its conformity to or compliance with State, Federal and local statutes, regulations, ordinances or instructions; the Contractor will be liable for the cost associated with loss of conformity or compliance.

The Contractor understands the cost reflects violation fines identified by the Michigan Social Security Number Privacy Act, 454 of 2004 and the Michigan Identity Theft Protection Act, Act 452 of 2004 as amended.

XI. Effective Date

These Safeguard requirements will be reviewed whenever the Contract modifications include specifications or processes that affect tax data.

Attachment A

Reset Form

Michigan Department of Treasury
3337 (Rev. 10-16)

Vendor, Contractor or Subcontractor Confidentiality Agreement

The Revenue Act, Public Act 122 of 1941, MCL 205.28(1)(f), the City Income Tax Act, Public Act 284 of 1964, MCL 141.674(1), and Internal Revenue Code (IRC) 6103(d), make all information acquired in administering taxes confidential. The Acts and IRC hold a vendor, contractor or subcontractor and their employees who sell a product or provide a service to the Michigan Department of Treasury, or who access Treasury data, to the strict confidentiality provisions of the Acts and IRC. Confidential tax information includes, but is not limited to, information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the Michigan Department of Treasury for a tax administered by the department.

INSTRUCTIONS. Read this entire form before you sign it. If you do not complete this agreement, you will be denied access to Michigan Department of Treasury and federal tax information. After you and your witness sign and date this form, keep a copy for your records. Send the original to the address listed below.

Company Name and Address (Street or RR#, City, State, ZIP Code)		Last Name	First Name
		Driver License Number/Passport Number	Telephone Number
State of Michigan Department	Division	Subcontractor Name if Product/Service Furnished to Contractor	
Describe here or in a separate attachment the product or service being provided to the State of Michigan Agency (Required).			

Confidentiality Provisions. It is illegal to reveal or browse, except as authorized:

- All tax return information obtained in connection with the administration of a tax. This includes information from a tax return or audit and any information about the selection of a return for audit, assessment or collection, or parameters or tolerances for processing returns.
- All Michigan Department of Treasury or federal tax returns or tax return information made available, including information marked "Official Use Only". Tax returns or tax return information shall not be divulged or made known in any manner to any person except as may be needed to perform official duties. Access to Treasury or federal tax information, in paper or electronic form, is allowed on a **need-to-know** basis only. Before you disclose returns or return information to other employees in your organization, they must be authorized by Michigan Department of Treasury to receive the information to perform their official duties.
- Confidential information shall not be disclosed by a department employee to confirm information made public by another party or source which is part of any public record. 1999 AC, R 2005.1004(1).

Violating confidentiality laws is a felony, with penalties as described:

Michigan Penalties
MCL 205.28(1)(f) provides that you may not willfully disclose or browse any Michigan tax return or information contained in a return. Browsing is defined as examining a return or return information acquired without authorization and without a **need to know** the information to perform official duties. Violators are guilty of a **felony** and subject to **fines of $5,000 or imprisonment for five years, or both**. State employees will be discharged from state service upon conviction.

Any person who violates any other provision of the Revenue Act, MCL 205.1, et seq., or any statute administered under the Revenue Act, will be guilty of a misdemeanor and **fined $1,000 or imprisonment for one year, or both**, MCL 205.27(4).

City Penalties
MCL 141.674(2) provides that any person divulging confidential City Tax information is guilty of a misdemeanor and subject to a fine not exceeding $500 or imprisonment for a period not exceeding 90 days, or both, for each offense.

Federal Penalties
If you willfully disclose federal tax returns or tax return information to a third party, you are guilty of a **felony with a fine of $5,000 or imprisonment for five years, or both, plus prosecution costs** according to the Internal Revenue Code (IRC) §7213, 26 USC 7213.

In addition, inspecting, browsing or looking at a federal tax return or tax return information without authorization is a **felony violation** of IRC §7213A subjecting the violator to a **$1,000 fine or imprisonment for one year, or both, plus prosecution costs**. Taxpayers affected by violations of §7213A must be notified by the government and may bring a civil action against the federal government and the violator within two years of the violation. Civil damages are the **greater of $1,000 or actual damages** incurred by the taxpayer, plus the costs associated with bringing the action, 26 USC 7431.

Failure to comply with this confidentiality agreement may jeopardize your employer's contract with the Michigan Department of Treasury.

Certification		
By signing this Agreement, I certify that I have read the above confidentiality provisions and understand that failure to comply is a felony.		
Print name of employee signing this agreement	Signature of person named above	Date signed
Print Witness Name (Required)	Signature of Witness (Required)	Date signed

Submit your form to the following address:
Office of Privacy and Security/ Disclosure Unit
Michigan Department of Treasury
430 W. Allegan Street
Lansing, MI 48922

Questions, contact the **Office of Privacy and Security by telephone, 517-636-4239; fax, 517-636-5340; or email:**
Treas_Disclosure@michigan.gov

Attachment B

Michigan Department of Treasury
4000 (Rev. 05-14)

Reset Form

Incident Report

INSTRUCTIONS: Complete Parts 1 and 2 and immediately submit Initial Report to the Office of Privacy and Security. After incident resolution, submit Final Report (Parts 1, 2 and 3) to the Office of Privacy and Security. Refer to Procedure PT-03253, Incident Reporting and Handling.

PART 1: A. CONTACT INFORMATION (Reporting Entity)

Full Name (Last, First, Middle Initial)	Division/Office	
Telephone Number	Fax Number	E-Mail Address

B. CONTACT INFORMATION (Affected Entity)

Full Name (Last, First, Middle Initial)	Division/Office	
Telephone Number	Fax Number	E-Mail Address

PART 2: INCIDENT INFORMATION

Whose information was involved in the incident?

☐ Treasury ☐ Federal Tax Information ☐ Other State Agency, specify _____ ☐ Other _____

Incident Category (select all that apply)

☐ Passwords Shared/Stolen	☐ Computer Virus/Spam	☐ Paper Archives Compromised
☐ Misrouted Communications	☐ Data Destruction/Deletion	☐ Safe/Lockbox/other Compromise
☐ Unauthorized Access	☐ Backups Missing or Stolen	☐ Delivery of Documents Lost
☐ Fraudulent Actions	☐ Hacking of Networks/Systems	☐ Inappropriate Destruction Paper
☐ Lost/Stolen Information/Data	☐ Improperly Secured Sys/Web	☐ Inappropriate Destruction Media
☐ Lost/Stolen Cash/Checks	☐ Circumvention of Security Protocols	☐ Lost/Stolen Equipment
☐ Inappropriate Building Access	☐ _____	☐ _____

Incident Affects

☐ Financial Information/Resources	☐ Personal Information (SSN, Driver License No. Financial information)	☐ Unauthorized/Unlawful Activity
☐ Confidential/Sensitive Information	☐ Human Resources (threat)	☐ Other _____

Date Incident Occurred	Time Incident Occurred	Date Incident Discovered	Time Incident Discovered

Incident Location	Number of Individuals Affected

Involved Parties/Entities	Does this involve personal information (first and last name along with a SSN, driver license number, or credit/debit card account number)? ☐ Yes ☐ No

Date of Initial Report

Description of Incident

PART 1: CONTACT INFORMATION (Affected Entity)

Full Name (Last, First, Middle Initial)	Division/Office

PART 3: INCIDENT RESOLUTION

Notification issued to affected individuals?	How many notifications were sent?	Breach Notification Method?
☐ Yes ☐ No		☐ E-mail ☐ Telephone ☐ US Mail ☐ Web

Who was notified?	Date notification was issued

Incident Cost

☐ Check if incident costs are less than $250. If $250 or more, complete the detailed summary of costs below.

Manhours:

Treasury $_____

DTMB-OES $_____

DTMB-Treasury Agency Services $_____

Other:

Postage $_____

Credit Monitoring Service $_____

_____ $_____

Total Cost of Incident $_____

Action Taken

Incident Impact

Post Incident Recommendations

PART 4: REPORT PREPARER INFORMATION

Final Report Prepared By:	Date Prepared	Preparer Title	Preparer's Telephone Number

Preparer Signature	Date

OFFICE OF PRIVACY AND SECURITY USE ONLY

Administrator, Office of Privacy and Security Signature	Date

SCHEDULE G – TRANSITION IN AND OUT PLANS

Transition-In and Transition-Out Plan

This plan details the structured approach for a seamless transition into Contractor's solution and a subsequent transition out to a third-party solution if required. The goal is to minimize disruption, maintain service continuity, and ensure the integrity of all data and processes. This plan is based on a standard 90-day timeline for both phases, which can be adjusted based on the project's complexity.

Transition-In Plan

The transition-in phase is designed to systematically replace the current system with the Contractor's solution. This phase involves close collaboration with the State to ensure a smooth and effective migration.

Timeline and Key Activities

Phase	Duration	Activities
Phase 1: Planning & Discovery	Weeks 1-4	• Project Kick-off Meeting • Team Introductions & Roles Defined • Detailed Project Plan Finalized • Current State Assessment • Requirements Validation • Data Migration Strategy Defined
Phase 2: Execution & Configuration	Weeks 5-10	• System Configuration & Customization • Data Extraction from Legacy System • Data Cleansing & Mapping • Initial Data Migration Test Run • User Acceptance Testing (UAT) Environment Setup • Training Program Development
Phase 3: Deployment & Go-Live	Weeks 11-12	• Final Data Migration • End-User Training • System Go-Live • Post-Implementation Support

Deliverables

- Project Kick-off Deck: Outlines project scope, objectives, and team roles.
- Detailed Project Plan: Comprehensive work breakdown structure, schedule, and resource allocation.
- Data Migration Strategy: A document detailing the approach, tools, and schedule for data transfer.
- User Acceptance Testing (UAT) Plan: Scripts and procedures for testing the new system.
- Training Materials & Schedule: Guides and presentations for end-users.
- Go-Live Checklist: A pre-deployment checklist to ensure all tasks are completed.
- Post-Implementation Report: Summary of the transition, including lessons learned.

State Participation

- Project Sponsor: The State will designate a Project Sponsor to provide overall guidance and decision-making authority.
- Subject Matter Experts (SMEs): The State will provide SMEs to validate requirements, assist with data mapping, and participate in UAT.
- IT Team: The State's IT team will provide access to the legacy system and support for network and security configurations.
- End-Users: State end-users will participate in training and UAT to ensure a smooth adoption of the new system.
- Data Owner: The State will designate a data owner to approve the final data migration and confirm data integrity.

Risk Mitigation Strategies

Risk	Mitigation Strategy
Data Corruption/Loss	• Perform a full data backup before migration • Conduct multiple test migrations. • The State's Data Owner will validate a sample of the migrated data. • Maintain the legacy system in a read-only state for a defined period.
User Resistance	• Engage users early in the process through training and UAT • Provide comprehensive, role-specific training. • Offer a dedicated help desk for the first 30 days post-go-live.
Schedule Delays	• Establish a clear communication plan with weekly status reports • Hold regular meetings to track progress and identify roadblocks early • The project plan includes contingency buffers for unexpected issues.
Integration Failure	• Test all third-party integrations in a sandbox environment before final deployment. • Work with the State's IT team to ensure all API and security requirements are met.

Transition-Out Plan

The transition-out phase is designed to provide a comprehensive, organized, and cooperative process for migrating from the Armedia's solution to a new third-party solution.

Timeline and Key Activities

Phase	Duration	Activities
Phase 1: Knowledge Transfer	Weeks 1-4	• Identify key personnel for knowledge transfer. • Provide comprehensive system documentation. • Hold transfer sessions for system configuration, business rules, and technical architecture.

Phase 2: Data & Asset Transfer	Weeks 5-10	• Document data schema and data models. • Extract and deliver all State data in an agreed-upon format. • Provide access to archived data and system logs. • Hand over all intellectual property and configurable assets.
Phase 3: Decommissioning	Weeks 11-12	• Assist the State's IT team with data validation. • Confirm all deliverables have been accepted by the State. • Decommission the system and securely delete State data from the Armedia's infrastructure.

Deliverables

- Final System Documentation: A complete set of updated documentation, including technical manuals and user guides.
- Data Archive: All State data extracted and delivered in a defined format (e.g., CSV, SQL dump).
- Decommissioning Plan: A step-by-step guide for safely and securely shutting down the system.
- Transition-Out Report: A final report confirming the completion of all tasks and deliverables.

State Participation

- Transition Lead: The State will appoint a Transition Lead to coordinate all transition-out activities.
- Technical Team: The State's technical team will be responsible for receiving and validating the transferred data and documentation.
- Acceptance Committee: The State will form a committee to formally accept all transition deliverables.

Risk Mitigation Strategies

Risk	Mitigation Strategy
Loss of Institutional Knowledge	• Create a structured knowledge transfer plan with defined milestones. • Provide complete and well-organized documentation and conduct dedicated transfer sessions.
Data Integrity Issues	• Extract data in a verifiable format. • The State's technical team will validate the integrity of the transferred data before the system is decommissioned.
Access Delays	• Maintain access to the Armedia's solution for a defined period after the main transition-out to allow for data validation and final checks.