



STATE OF MICHIGAN PROCUREMENT
 Department of Technology, Management & Budget
 320 S. Walnut Street, Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **171-230000000919**

between
 THE STATE OF MICHIGAN
 and

CONTRACTOR	Kaseware, Inc.
	191 University Blvd., Suite 170
	Denver, Colorado 80206
	Mark Dodge
	734-474-4786
	Mark.dodge@kaseware.com
	VS0094916

STATE	Program Manager	Various	MDOS
	Contract Administrator	Jeremy Lyon	DTMB
		517-230-2858	
		LyonJ5@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Case Management System			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
6/6/2023	6/5/2028	5-1 Year	N/A
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card	<input type="checkbox"/> Payment Request (PRC)	<input type="checkbox"/> Other	<input type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
New MA established from RFP# 220000002580.			
AD Board Approval 6/6/2023			

ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION

\$420,000

CONTRACT NO. 171-2300000000919

Program Managers

Agency	Name	Phone	Email
MDOS	Peggy Hines	517-230-3514	HinesP@Mchigan.gov
DTMB	Dan Klodt	517-930-3506	KlodtD@michigan.gov

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

Agency

Date

SOFTWARE CONTRACT TERMS

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 Kaseware, Inc. (“**Contractor**”), a Delaware CORPORATION. This Contract is effective on 5/22/2023 (“**Effective Date**”), and unless terminated, will expire on 5/21/2028 (the “**Term**”).

This Contract may be renewed for up to 5 additional, 1-year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via Contract 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 accordance with **Section 9.1** and a Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

“**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 17.2(b)**.

“**Third Party Components**” means all third party 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 Bid Response or as part of the State’s Security Accreditation Process defined in Schedule E – Data Security Schedule.

“**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.

“Background Technology” means all Software, data, know-how, ideas, methodologies, specifications, and other technology in which Contractor owns such Intellectual Property Rights as are necessary for Contractor to grant the rights and licenses set forth in **Section 5**, and for the State (including its Authorized Users, licensees, successors and assigns) to exercise such rights and licenses, without violating any right of any Third Party or any law or incurring any payment obligation to any Third Party. Background Technology must: (a) be identified as Background Technology in the Statement of Work; and (b) have been developed or otherwise acquired by Contractor prior to the date of the RFP.

“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” has the meaning set forth in **Section 2.2**.

“Change Notice” has the meaning set forth in **Section 2.2(b)**.

“Change Proposal” has the meaning set forth in **Section 2.2(a)**.

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

“Confidential Information” has the meaning set forth in **Section 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 a Statement of Work.

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

“Contractor’s Bid Response” means the Contractor’s proposal submitted in

response to the RFP.

“Contractor Hosted” means the Hosted Services 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 a Statement of Work to serve as the primary contact with regard to services, 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, 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**.

“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 Software.

“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 **Section 23.1**.

“Harmful Code” means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to

destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

“HIPAA” has the meaning set forth in **Section 21.1**.

“Hosted Services” means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic 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 9.2(a)**.

“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 the Software to conform to the requirements of this Contract, including any applicable Documentation.

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

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

“PAT” means a document or product accessibility template, including any

Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

“Permitted Subcontractor” means any third party hired by Contractor to perform Services for the State under this Contract or have access to State Data.

“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.

“RFP” means the State's request for proposal designed to solicit responses for Services under this Contract.

“Services” means any of the services, including but not limited to, Hosted Services, 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 the physical location designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Software.

“Software” means Contractor's software as set forth in a Statement of Work, and any 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.

“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, RFP 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 21.1**.

“State Hosted” means the Hosted Services are not provided by Contractor or one or more of its Permitted Subcontractors.

“State Materials” means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, 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 Software and other Deliverables; and (c) perform other duties as may be specified in a Statement of Work Program Managers will be identified in a Statement of Work.

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

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

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

“Testing Period” has the meaning set forth in **Section 9.1(b)**.

“Transition Period” has the meaning set forth in **Section 16.3**.

“Transition Responsibilities” has the meaning set forth in **Section 16.3**.

“Unauthorized Removal” has the meaning set forth in **Section 2.5(b)**.

“Unauthorized Removal Credit” has the meaning set forth in **Section 2.5(c)**.

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

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

“WCAG 2.0 Level AA” means level AA of the World Wide Web Consortium Web Content Accessibility Guidelines version 2.0.

“Work Product” means all State-specific deliverables that Contractor is required to, or otherwise does, provide only 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. Work Product does not include Background Technology or Software modifications or enhancements made available to all similarly situated users of the Software.

2. **Duties of Contractor.** Contractor will provide Services and Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Services and Deliverables 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 a Statement of Work, including changes to the Services and Implementation Plan (each, a **“Change”**). Upon the State’s submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 2.2**.

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

- (i) a written description of the proposed Changes to any Services or

Deliverables;

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

(b) Within 30 Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to a Statement of Work to which it relates; and

(c) 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 the Services under a Statement of Work without the Change;
- (ii) require Contractor to continue to negotiate a Change Notice;
- (iii) initiate a Dispute Resolution Procedure; or
- (iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Section 16.1** if the State's proposed modification is required by law.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of

Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities 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. Contractor Project Manager will be identified in a Statement of Work.

- (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;
- (ii) the State consents in writing to any removal requested by Contractor in writing;
- (iii) Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Contractor Project Manager on the occurrence of any event set forth in **Section 2.4(c)**. Such replacement will be subject to the State's prior written approval.

2.5 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State Program Managers or their designees, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness,

disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 16.1**.

(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 \$10,000 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. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. 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 Services or Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) name the State a third-party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;

(c) be responsible for all fees and expenses payable to, by or on behalf of each 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

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental 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 actually 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:
Jeremy Lyon 320 S. Walnut Lansing, MI 48933 LyonJ5@michigan.gov 517-230-2858	Kaseware, Inc 191 University Blvd. #170 Denver, Colorado 80206 salesteam@kaseware.com +1 720-507-9133.

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

5. **Intellectual Property Licenses.**

5.1 **Subscription License.** If the Software is Contractor Hosted and Contractor is providing the State access to use its Software during the Term of the Contract only, then:

(a) Contractor hereby grants to the State, exercisable by and through its Authorized Users, a nonexclusive, royalty-free, irrevocable right and license during the Term and such additional periods, if any, as Contractor is required to perform Services under this Contract or any Statement of Work, to:

- (i) access and use the Software, including in operation with other software, hardware, systems, networks and services, for the State's business 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 **Section 5.2(c)** below.

(b) License 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.

(c) Use. 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.

5.2 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 5**. 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.

5.3 Non-Software Deliverables license. To the extent the State does not own a non-Software Deliverable, or any other output generated by use of the Software,

Contractor hereby grants the State a non-exclusive, non-transferable, non-sublicensable, worldwide, royalty-free license to all non-Software Deliverables and output.

5.4 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.

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 **Section 7.1(c)**:

- (i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and
- (ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

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

arising therefrom or relating thereto.

7.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including 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, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

- (i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and
- (ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called “moral rights” or rights of *droit moral* with respect to the Work Product.

8. Software Implementation.

8.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise 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 Hosted Services are ready for use in a production environment, 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 in **Section 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 **Section 9.1**, **Section 9.4**, and **Section 9.5**.

(b) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity 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 Non-Conformity, 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 Non-Conformity in the tested Software.

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

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Non-Conformities, 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 Non-Conformities, on the completion of which the State will, as appropriate:

- (i) notify Contractor in writing of Non-Conformities 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 **Section 9.4** and **Section 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 Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in a Statement of Work. 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 **Section 9.1(a)** or **Section 9.3(c)(i)**, identifying any Non-Conformities.

9.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity 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 for cause in accordance with **Section 16.1**.

9.6 Acceptance. Acceptance (“**Acceptance**”) of the Software (subject, where applicable, to the State’s right to Integration Testing) and any Deliverables will occur on the date that is the earliest of the State’s delivery of a notice accepting the Software or Deliverables under **Section 9.3(b)**, or **Section 9.3(c)(ii)**.

10. **Non-Software Acceptance.**

10.1 All other non-Software Services and 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 Services and 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 Services and Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Services and Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the non-Software Services and Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16.1**, Termination for Cause.

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

10.3 If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or

in part. The State, or a third party identified by the State, may provide the non-Software Services and 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 to any other party without the prior 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 party. 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 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. **Invoices and Payment.**

13.1 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 Services and Deliverables provided as

specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 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 Services and 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.

13.3 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.

13.4 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.

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

13.6 Pricing/Fee Changes. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

(b) Excluding federal government charges and terms. Contractor warrants and agrees that each of the Fees, economic or product terms or warranties granted pursuant to this Contract are comparable to or better than the equivalent fees, economic or product term or warranty being offered to any commercial or government customer

(including any public educational institution within the State of Michigan) of Contractor. If Contractor enters into any arrangements with another customer of Contractor to

provide the products or services, available under this Contract, under more favorable prices, as the prices may be indicated on Contractor's current U.S. and International price list or comparable document, then this Contract will be deemed amended as of the date of such other arrangements to incorporate those more favorable prices, and Contractor will immediately notify the State of such Fee and formally memorialize the new pricing in a Change Notice.

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 under **Section 16.1** 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 Contract Activities, 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, if the State notifies Contractor of the breach and, in the State's reasonable discretion, Contractor fails to remedy the breach within 30 days of the State's notice. . 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 **Section 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 **Section 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 **Section 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 90 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 22.5 regarding 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

17.2 any negligent or otherwise more culpable 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). 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, under this **Section 17**, 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 Software 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 Software 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 Software 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 Software 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 Software without disruption.

18.4 If Contractor directs the State to cease using any Software under **Section 18.3**, the State may terminate this Contract for cause under **Section 16.1**. Unless the claim arose against the Software 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 Software by the State without the prior knowledge and approval of Contractor.

19. **Disclaimer of Damages and Limitation of Liability.**

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

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

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; and

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

- (i) personally identifiable information (“**PII**”) collected, used, Processed, stored, or generated as the result of the Services, 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 Services, which is defined under the Health Insurance Portability and Accountability Act (“**HIPAA**”) and its related rules and regulations.
- (iii) Criminal Justice information as defined in the FBI CJIS Security Policy and the Michigan CJIS Administrative Rules.

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 Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. 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 Services, 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 continental United States and
- (d) not use, sell, rent, transfer, 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 Discovery. Contractor will immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Software and Hosted Services, if applicable. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. In no event will Contract provide such notification more than twenty-four (24) hours after Contractor receives 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 and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for State review, revision and approval.

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 relating to a breach of **Section 21.6** 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 by, through, or on behalf of, the receiving party). 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

22.3 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 **Section 22.2**.

22.4 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.

22.5 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.

22.6 Surrender of Confidential Information upon Termination. 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, 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 Services for the Software, 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 with its actual or required performance of the Services, 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 all uses of the Software permitted 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 all uses of the Software 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 Updates. Contractor will provide the State, at no additional charge, adequate Documentation for use of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State for material changes only. Contractor will provide no less than five business days advance notice for all major updates as well as a walkthrough of any big changes to the software.

28. **Source Code Escrow**

28.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release.

28.2 Deposit. Within 30 business days of the Effective Date, Contractor will deposit with the escrow agent, pursuant to the procedures of the escrow agreement, the Source Code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. Promptly after release of any update, upgrade, patch, bug fix, enhancement, new version, or other revision to the resume contact information with the escrow agent.

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

- (a) Contractor will promptly deposit conforming Deposit Material; and
- (b) Contractor will pay the escrow agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this **Section 28.3** will constitute material breach of this Contract, and no further payments will be due from the State until such breach is cured, in addition to other remedies the State may have.

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

29. **Contractor Representations and Warranties.**

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

- (a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;
- (b) It has the full right, power, and authority to enter into this Contract, to grant

the rights and licenses granted under 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 RFP; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

(c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous 5 years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

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

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

(a) it 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;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) it 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;

(d) 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;

(e) 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;

(f) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as 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;

(g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:

- (i) Harmful Code; or
- (ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Third Party Components specifically described in a Statement of Work or later disclosed if Contractor modifies the Software.

(h) 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

(i) it 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.

(j) 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;

(k) 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;

(l) 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.

(m) 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.

(n) If Contractor Hosted:

(i) Contractor will not advertise through the Hosted Services (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 Software and Services 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 Hosted Services 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 Hosted Services have any material undocumented feature;

(o) 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 Software or with the Hosted Services, if applicable, 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 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. **Offers of Employment.** During the first 12 months of the Contract, should Contractor hire an employee of the State, without prior written consent of the State, who has substantially worked on any project covered by this Contract. The Contractor will be billed for 50% of the employee's annual salary in effect at the time of separation.

31. **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; 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 Services and Deliverables in connection with this Contract.

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

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 (as defined in Executive Directive [2019-09](#)), 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 any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

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

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

36. **Force Majeure**

36.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, 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 Hosted Services 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 Hosted Services; 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 **Sections 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 makes a determination 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 through transactions with MiDEAL members, and other states (including governmental subdivisions and authorized entities). Payments under this Contract will not require payment of an administrative fee. 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 <https://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 except by signed agreement between the parties (a “**Contract Change Notice**”). Notwithstanding the foregoing, no subsequent Statement of Work or Contract 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. **HIPAA Compliance.** To the extent applicable, the State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.

46. **Accessibility Requirements.**

46.1 All Software provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA. Contractor must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for each product provided under the Contract. At a minimum, Contractor must comply with the WCAG 2.0 Level AA conformance claims it made to the State, including the level of conformance provided in any PAT. Throughout the Term of the Contract, Contractor must:

(a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;

(b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;

(c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor’s Software to WCAG 2.0 Level AA;

(d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor’s Software;

(e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and

(f) participate in the State of Michigan Digital Standards Review described below.

46.2 State of Michigan Digital Standards Review. Contractor must assist the State, at no additional cost, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to validate Contractor's accessibility and compliance with WCAG 2.0 Level AA. Prior to the solution going-live and thereafter on an annual basis, or as otherwise required by the State, re-assessment of accessibility may be required. At no additional cost, Contractor must remediate all issues identified from any assessment of accessibility pursuant to plans and timelines that are approved in writing by the State.

46.3 Warranty. Contractor warrants that all WCAG 2.0 Level AA conformance claims made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to the State, are true and correct. If the State determines such conformance claims provided by the Contractor represent a higher level of conformance than what is actually provided to the State, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated WCAG 2.0 Level AA conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in addition to all other remedies available to the State, the State may terminate this Contract for cause under **Section 16.1**.

46.4 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

46.5 Failure to comply with the requirements in this **Section 47** shall constitute a material breach of this Contract.

47. **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.

48. **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.

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

50. **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.

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 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. 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 Software and 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 Software and other 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 Software or other Deliverables, and the same, if not already in the State's possession, 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

This schedule identifies the requirements of the Contract.

1. DEFINITIONS

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

Term and Acronyms	Definition
EASA	Enterprise Architecture Solution Assessment; All vendor proposals and new contracts must be accompanied by an Assessment, documenting the architectural details of the proposed solution.
SOM	State of Michigan
SSP	System Security Plan; Overview of the information system and security requirements including information assets, security categorization, applicable laws and regulations, system interconnections, information sharing, system dependencies, network diagrams, network devices and components, system hardware, system software, data flow diagrams, implementation of the security controls, Describes the controls in place or planned to be in place required to provide the appropriate level of security.

2. BACKGROUND

The Office of Investigative Services (OIS) investigates and opens cases regarding fraudulent, improper, or suspicious activity involving any Michigan Department of State programs or documents. The OIS is the official point of contact for law enforcement agencies investigating reports of fraud and ensuring compliance with programs administered by the Michigan Department of State. This Contract supports the implementation and support of an OIS IT solution for investigative case management.

3. PURPOSE

The State is contracting with Contractor for a Hosted solution and applicable Services.

The State is contracting for Contractor to implement a new solution to support enforcement case management tasks for OIS-Enforcement Division staff. The Enforcement Division case management system will provide a means for assigning case numbers for incoming complaints, serve as a repository for core case investigation information, development of narrative reports, provide case routing and assignment and approval routing and allow for statistical information to be generated from the system.

Single sign-on capability for system access will also be part of the solution. The solution will provide evidence logging capability, templates generated as part of the solution's Go Live, as well as functionality for searching, sorting, and prioritizing of enforcement cases.

4. IT ENVIRONMENT RESPONSIBILITIES

The solution will be hosted and managed by the Contractor's Microsoft Azure Government Cloud which maintains a FedRAMP High P-ATO. Contractor adheres to and exceeds CJIS standards. Contractor will regularly leverage independent audits and maintain compliance with SOC 2 Type 2.

Contractor will comply with Schedule E, Attachment 1 and the States PSPs. Contractor has completed CJIS audits for law enforcement agencies. Contractor is CJIS compliant. The audit reports are not available to Contractor for dissemination. Data at rest in the Contractor's application is encrypted on Microsoft Azure Cloud using 256 bit AES encryption which is FIPS 140-2 compliant. Data in transit is encrypted using Ubuntu Open SSL Cryptographic Module which is FIPS 140-2 compliant.

Contractor's Disaster Recovery Plan is found in Schedule F which includes but is not limited to the following requirements:

- Back-up and Recovery:
 - Organization policy and procedures authorizing this activity.
 - The roles and responsibilities within the organization and the integration of activities with any affiliated organizations also responsible for back-up and recovery.
 - Training and awareness of staff and contractors.
 - The most recent back up/fail-over test date at the time of submission.
 - Priority for the recovery and reconstitution of activities.
- Incident Handling:
 - Organization policy and procedures authorizing this activity and covers the areas of preparation, detection and analysis, containment, eradication, and recovery.
 - Roles and responsibilities with the organization and affiliated organizations.
 - Training and awareness of staff and contractors.
 - Description of the implementation of secure communications such as a description of software tool(s) used for tracking and documenting the incident or disaster.
- Disaster Recovery Planning:
 - Identification of the organization's business functions, recovery objectives, restoration priorities, and metrics of evaluation.
 - Organization policy and procedures authorizing this activity and covers the areas of preparation, detection and analysis, containment, eradication, and recovery.

- Roles and responsibilities with the organization and affiliated organizations.
- Training and awareness practices of staff and contractors.
- The most recent disaster recovery/contingency plan test date at time of submission.
- Methods used to identify deficiencies and corrective actions from the most recent disaster/contingency plan test and the status of corrective actions.
- Description of the implementation of secure communications such as a description of software tool(s) used for tracking and documenting the incident or disaster.
- Identification and use of alternate storage and process sites for business continuity.
- Protections and recovery planning for ransomware attacks.

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	Identify contract components with contractor or subcontractor name(s), if applicable
-------------------------	--

Facilities	Microsoft Azure
Infrastructure	Microsoft Azure
Platform	Kaseware and Microsoft Azure
Application	Kaseware and Microsoft Azure
Storage	Microsoft Azure
Backup	Microsoft Azure
Development	Kaseware

Contractor's Solution is hosted on Microsoft Azure Gov. Cloud. Azure is considered a subcontractor.

For integration testing and data migration efforts, Contractor may require access to, or anonymized copies of, State Data.

5. 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 Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

Contractor complies with WCAG 2.0 Level AA and will meet all requirements of ADA.

6. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
State Employee (including contractors)	Read, Write, Administrative	50	50

Contractor solution must support the number of concurrent Users identified above.

No equipment is needed from the State as Contractor is hosted on Microsoft Azure Government Cloud.

7. ACCESS CONTROL AND AUTHENTICATION

The Contractor's solution must integrate with the State's IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy ([MILogin - Help \(michigan.gov\)](https://michigan.gov/milogin)), which consist of:

7.1 MILogin/Michigan Identity, Credential, and Access Management (MICAM). An enterprise single sign-on and identity management solution based on IBM's Identity and Access Management products including, IBM Security Identity Manager (ISIM), IBM Security Access Manager for Web (ISAM), IBM Tivoli Federated Identity Manager (TFIM), IBM Security Access Manager for Mobile (ISAMM), and IBM DataPower, which enables the State to establish, manage, and authenticate user identities for the State's Information Technology (IT) systems.

7.2 MILogin Identity Federation. Allows federated single sign-on (SSO) for business partners, as well as citizen-based applications.

7.3 MILogin Multi Factor Authentication (MFA, based on system data classification requirements). Required for those applications where data classification is Confidential and Restricted as defined by the 1340.00 Michigan Information Technology Information Security Policy (i.e. the proposed solution must comply with PHI, PCI, CJIS, IRS, and other standards).

7.4 MILogin Identity Proofing Services (based on system data classification requirements). A system that verifies individual's identities before the State allows access to its IT system. This service is based on "life history" or transaction information aggregated from public and proprietary data sources. A leading credit bureau provides this service.

Contractor will integrate with MILogin, the state's SSO solution.

8. DATA RETENTION AND REMOVAL

The Contractor will provide the State with the ability to do the following, at no additional cost to the State:

1. Retain all data for the entire length of the Contract unless otherwise direct by the State;
2. Delete data, even data that may be stored off-line or in backups; and
3. Retrieve data, even data that may be stored off-line or in backups.

Contractor's Software, allows the State record managers to be able to design retention rules in the software based on system configurations and data attributes Solution's includes.

9. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM, with supporting platforms, 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 with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers and the state standard browser without the use of special plugins or extensions. The rules used to base the minimum browser requirements include:

- Over 2% of desktop and mobile & tablet site traffic, measured using Michigan.gov sessions statistics and
- The current browser identified and approved as the State of Michigan standard

This information can be found at <https://www.michigan.gov/browserstats>. Please use the most recent calendar quarter to determine browser statistics. For those desktop and mobile & tablet browsers with over 2% of site traffic, , the current browser version as well as the previous two major versions must be supported.

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

Contractor solution is hosted on Microsoft Azure Government Cloud. Contractor will provide any necessary plug-ins at no extra cost to the State.

10. SOFTWARE

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet**.

Contractor must provide a list of any third party components, and open source component included with or used in connection with the deliverables defined within this Contract. This information must be provided to the State on a quarterly basis and/or if a new third party or open source component is used in the performance of this Contract.

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.

SOM IT Environment Access

Contractor must access State environments using one or more of the following methods:

- State provided VDI (Virtual Desktop Infrastructure) where compliant.
- State provided and managed workstation device.
- Contractor owned and managed workstation maintained to all State policies and standards.
- Contractor required interface with State systems which must be maintained in compliance with State policies and standards as set forth in **Schedule E – Data Security Requirements**.
- From locations within the United States and jurisdiction territories.

Name: Kaseware Type: SaaS Version: 4.0

Release: 4.0

Architecture: Contractor's detailed system architecture models can be shared under Non-Disclosure Agreement.

Open-Source Intelligence (OSINT)

The Software must include Open-Source Intelligence (OSINT) integrations to Shadow Dragon products including SocialNet and OIMonitor. The Software must give authorized users the ability to search over 115+ social media platforms by name, alias, email, and phone number directly through the Software's graphing tools. The Software must allow authorized users to automatically generate links between data points and perform de-duplication processes. The Software should include integration options with PowerBI at no additional cost. The Software should include options with the following integrations at an additional cost.

Available Integrations

- SocialNet
- OIMonitor
- eGuardian
- Jira
- LDAP
- Tableau
- Splunk

Contractor utilizes dozens of third-party components as part of the solution. The following are some of the major third-party components:

- Microsoft Azure
- Kubernetes
- Hazelcast
- Docker
- ExtJS
- Java
- Apache
- MetaBase
- PostgreSQL
- ArangoDB
- GraphQL

Contractor Software must run on any mobile device that has a browser or has the ability to install an iOS native and Android native app.

The following features are available on a mobile device:

- Search Capability
- Note Taking
- Photo and Video Capture with Upload Capabilities
- Barcode Scanning
- Evidence Lookup
- Case Lookup and Review

11. INTEGRATION

Contractor must integrate their solution to the following technologies:

Current Technology	MILogin - we support these types of authentication: HTTP Header Federation Technology SAML OAUTH Other
Volume of Data	Unknown at this time
Format of the input & export files	N/A
Contractor solution includes a large set of GraphQL APIs that are included with the software. Customers can leverage the APIs in the solution to create, update, and extract data from all	

solution features through our APIs. Contractor commonly integrates the solution to Single Sign On (SSO) providers and have included integration through a SAML2.0 protocol.	
Current Technology	CARS (for validating information) - MDOS
Volume of Data	Unknown at this time
Format of the input & export files	N/A
Current Technology	CARS (for importing reports) - MDOS
Volume of Data	Unknown at this time
Format of the input & export files	N/A
Contractor will use GraphQL, CSV data import and if needed custom HTTP endpoints in order to perform needed integrations. Contractor will conduct analysis of the CARS system and select the appropriate tools and approach for the integration, understanding that the appropriate tools will be at no additional cost to the State.	

12. MIGRATION

Contractor must migrate the data identified in the table below:

Current Technology	MQ SQL
Data Format relative to the database technology used.	MS Office VBA
Number of data fields to give Contractor awareness of the size of the schema.	No views and No stored procedures. Approximately 40 tables and 100+ existing queries. No limit on users creating new tables, queries, reports.
Volume of Data	No views and No stored procedures. Approximately 40 tables and 100+ existing queries. No limit on users creating new tables, queries, reports. New system should only allow authorized users to create new reports and only the vendor should create new tables.
Database current size.	Under 10GB

Data Migration Services

The Contractor will complete data migration analysis on the State's existing data and determine a data migration approach. The Contractor will complete data migration testing and validate migrated data at no additional cost to the State.

Contractor's Data Migration Approach

Discovery

- Data Migration Analysis - Data will be analyzed to determine the level of effort (LOE) for the migration. A data migration Preparatory Questionnaire will be completed by the Contractor to assist with the information needed. To get a better understanding of the data during this step, it's very helpful to provide a database schema.

The following tasks will be completed by the Contractor for data migration preparation:

- Data Migration Kickoff
- SFTP Set-Up and Data Transfer - The Contractor team will set up an SFTP server to upload the data and attachments.
- Internal Data Review - The Contractor team will review data internally and identify questions and areas of improvement regarding the data

- Client Data Review - The Contractor team and the State team will meet as many times as necessary to discuss each column and determine if, how, and where each column will be imported.

Test and Execute

- Initial Sample Import: Once each of the fields have been reviewed, the Contractor team will upload a portion or sample of the data into the import tool and will map each column to a field in Contractor solution.
- Initial Sample Import Review: After all of the fields have been mapped, the Contractor team will test importing in a very small subset of data and will review that data with the State's stakeholders. Changes will be made, and once all of the stakeholders have agreed that the subset looks acceptable, the remainder of the sample data will be imported.
- Full Sample Import Testing and Signoff: At that time, the State will review and test the data to ensure it has the expected information. Once acceptable, the client will provide written confirmation that the data can be imported into the production system.
- Production Data Import: Once the data has been signed off on, the Contractor team will copy the import profiles into the production tenant and import the data.

The database may be increased at the time of transition, if required by the State, at no additional cost.

13. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency. Training must include classroom and online options and be able to allow for at least 50 participants. Training must allow at least 5 Administrative User participants for administrative training. Training must be provided as otherwise indicated by MDOS and at no additional cost to the State.

Training Approach & Plan

- Pre-Kickoff: Prior to project kick-off, Contractor must work with the State to identify Software users to ensure the training reflects all user types.
- Kickoff and Business Analysis: Business process information will be incorporated into all training sessions as necessary.
- On-Site Classroom Training: Contractor will provide four days of onsite work by one Contractor technical trainer, unless otherwise requested by the State. This training will focus on the Software for each user group. On-Site and virtual class material will consist of the in-application Help Guide, power point presentations used for interactive training, and user guides specific to State business processes.
- Virtual Training: Contractor will provide virtual training to further support, User Acceptance Training, transition and solution Go-Live. Virtual training will also be conducted for any additional recurring training after go-live.

14. TRANSITION RESPONSIBILITIES

Contractor will comply with its Transition Plan set forth in Schedule G.

15. 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 provide the following materials to support the users of the solution:

- In-application Help Guide – Contractor must provide an in-application help guide that is updated as the software is updated. The help guide must provide users with clear instructions on how to utilize the features of the Software, support, and explanations on the technical and installation aspects of the Software.
- PowerPoint Presentations for Training – Contractor must develop PowerPoint Presentations for interactive training. End-users will be able to retain these presentations for future use and continued training. The PowerPoints will contain information on Software instructions, installation, use and other functionality notes.
- User guides – Contractor must create specific guides reflecting State business processes for all end users. The guides will contain detailed information on the software features and functionality and instructions on common questions and user scenarios. As new features and updates occur, Contractor must update State user guides accordingly.
- System Configuration Design Plan – Contractor must provide a document that details out the findings and requirements from the business analysis and discovery sessions.

16. ADDITIONAL PRODUCTS AND SERVICES

The State may purchase additional products & services offered by Contractor that are in scope of the original Contract via contract change notice and in compliance with SOM procurement policy.

17. 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
Name: Mark Dodge Address: 191 University Blvd., Suite 170 Denver, Colorado 80206 Phone: 734-474-4786 Email: mark.dodge@kaseware.com

Classification	Skill Set	Years of Experience
Director of Technical Operations	Project management, risk analysis, cloud expertise, container skills, configuration management and IT operations.	15+ Years
Principal Engineer and Product Manager	Project management,	20+ Years
Software Engineer	Computer programming and coding, software development, and agile methodology knowledge	10+ Years
Software Testing Engineer	Software testing and debugging, observability and agile knowledge methodology	10+ Years
Training Technical Lead	Project management, communication, schedule management, workflow process analysis, systems testing and training facilitation skills.	7+ Years

Customer Success Specialist	Communication, workflow process analysis, systems testing and training facilitation skills.	5+ Years
------------------------------------	--	-----------------

18. CONTRACTOR KEY PERSONNEL

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

Contractor
Name: Korinne Condie Address: 191 University Blvd., Suite 170 Denver, Colorado 80206 Phone: 720-551-7012 Email: korinne.condie@kaseware.com

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

Contractor
Name: Scott Schons Address: 191 University Blvd., Suite 170 Denver, Colorado 80206 Phone: 720-307-7901 Email: scott.schons@kaseware.com

Contractor Implementation Manager. Contractor to provide name of individual who will be responsible for day-to-day management of the overall solution. This position is responsible for assisting the Contract Project Manager in the installation, system integration, security, and database design needs.

Contractor
Name: Korinne Condie Address: 191 University Blvd., Suite 170 Denver, Colorado 80206 Phone: 720-551-7012 Email: korinne.condie@kaseware.com

Contractor Training Lead. Contractor to provide name of individual responsible for the planning and delivery of all training related to this contract. This person must have experience leading training efforts for similar size and scope projects, to include providing guidance on the appropriate training program/plan for the specific audience and education need

Contractor
Name: Sarah Crank Address: 191 University Blvd., Suite 170 Denver, Colorado 80206 Phone: 720-551-8430 Email: sarah.crank@kaseware.com

19. CONTRACTOR PERSONNEL REQUIREMENTS

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

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

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

Offshore Resources.

Contractor will not be using offshore resources. All resources will be onshore. Contractor must provide the requested material defined in the Background Checks section.

Disclosure of Subcontractors.

Contractor will be using Azure as a subcontractor.

20. STATE RESOURCES/RESPONSIBILITIES

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
Jeremy Lyon 517-230-2858 LyonJ5@michigan.gov

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

DTMB Program Manager
Dan Klodt 517-930-3506 KlodtD@michigan.gov

Agency Program Manager
Peggy Hines, Director, Enforcement Division OIS-MDOS 517-230-3514 HinesP@michigan.gov

21. 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.

The Contractor must attend the following meetings, at a location and time as identified by the state, at no additional cost to the State:

- Kick off meeting
- Project planning sessions
- SUITE tailoring sessions
- Discovery/Requirements and analysis meetings

- Ongoing collaborative team meetings to facilitate discovery and development are required. If Agile Scrum development approach is proposed, then all Scrum ceremonies, including daily Scrum, sprint planning, sprint reviews, sprint retrospectives, backlog grooming, and artifacts will be encouraged and expected.
- All other meetings needed to successfully implement the new system.
- Daily standup/JAD sessions, depending on approach
- Security plan assessment and review sessions

Contractor will conduct JAD sessions in parallel with the business analysis sessions. Contractor will use the appropriate analysis, configuration, training and testing meetings to showcase solution functionality and relevant features.

Contractor will conduct 2 days of on-site Business Analysis unless the State requires additional on-site Business Analysis to be completed at no additional cost to the State. On-site Business Analysis will begin no later than 15 days from the date of Project Kickoff, unless otherwise agreed to by the State. Contractor will provide the State with a System configuration design plan that outlines the findings of business analysis sessions, a plan for relevant System configurations, and a mutually agreed upon deployment schedule for the State team. If necessary, further sessions can be conducted virtually.

Contractor's Chief Security Officer and Technical team will meet with the State to develop and execute the security plan and assessment. Contractor will conduct and facilitate the appropriate discovery and analysis sessions for the data migration scope. This includes reviewing the data migration approach and requirements. Contractor will conduct and facilitate the appropriate discovery and analysis sessions for the integration scope. This includes reviewing the data migration approach and requirements. The customer success team will schedule a 30-minute, monthly meeting with the MDOS designated users and system administrators to review user needs and any enhancements that would lead to a greater level of customer success.

22. 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.

Contractor will provide and maintain a Project Control Document* for this project. This document will contain the following information:

- Project Milestone Updates and Milestone Timelines
- Recent Accomplishments
- Upcoming Objectives and Tasks
- Issues and Workarounds
- Risks and Mitigation Plans
- Updated Cost Schedule and Invoice to Date Report

23. 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.

SUITE's primary goal is the delivery of on-time, on-budget, quality systems that meet customer expectations. SUITE is based on industry best practices, including those identified in the Project Management Institute's PMBoK and the Capability Maturity Model Integration for Development. It was designed and implemented to standardize methodologies, processes, procedures, training, and tools for project management and systems development lifecycle management. It offers guidance for efficient, effective improvement across multiple process disciplines in the organization, improvements to best practices incorporated from earlier models, and a common, integrated vision of improvement for all project and system related elements.

While applying the SUITE framework through its methodologies is required, SUITE was not designed to add layers of complexity to project execution. There should be no additional costs from the Contractor, since it is expected that they are already following industry best practices which are at least similar to those that form SUITE's foundation.

SUITE's companion templates are used to document project progress or deliverables. In some cases, Contractors may have in place their own set of templates for similar use. Because SUITE can be tailored to fit specific projects, project teams and State project managers may decide to use the Contractor's provided templates, as long as they demonstrate fulfillment of the SUITE methodologies.

Project Initiation Phase - Contractor will work with MDOS to provide any information needed to initiate the project and properly scope out the required resources and expectations from the State. Contractor will be well versed in the expected outcomes of the project and will review the Contract multiple times prior to the Project Planning sessions.

Project Planning Phase - During the Project Planning sessions, Contractor will collaboratively work with MDOS to develop a project management plan that aligns with the project milestones and the expected outcomes for stakeholders.

Project Execution - Contractor will collaboratively work with and assist with the State to get the necessary approval for the project plan. Once approved, project kickoff gives Contractor and the State the ability to align on business objectives, timelines, costs, and any previously identified risks with the larger group of stakeholders. Preparation and planning for the SSP also begins during this phase.

Requirements Definition and Functional Design Stage - Contractor will conduct 2 days of on-site Business Analysis, after the Project Kickoff. The business analysis sessions will be in-depth discovery into the end users of the solutions, their processes, and how they intend to use the software. To complete the Business Analysis milestone, Contractor will provide the State with a System configuration design plan that outlines the findings of business analysis sessions, a plan for relevant System configurations, logical system flow, and a mutually agreed upon deployment schedule for the State team. If necessary, further sessions can be conducted virtually. The SSP starts to be created in this phase with stages 1.0-5.0.

System Design Stage - The Contractor customer ops and development team will collaboratively work to configure the tenant based on the System configuration design plan that was signed off by MDOS. Stakeholders will be given regular updates and insight into progress via the ongoing collaborative team meetings. This includes discovery and analysis for data migration and integration efforts. These meetings will serve as an agile feedback loop for the systems design. The SSP will be updated accordingly as well.

Construction and Testing Stage - As the system will be hosted and managed by Contractor's Microsoft Azure Government Cloud, minimum construction and no installation training efforts are required for the majority of the functionality. Staging for data migration executions and integration implementations will occur during this phase in accordance with the project plan. Progress will be reported on by Contractor via collaborative meetings with MDOS. Integration, system testing and user acceptance testing will be utilized as a feedback loop for construction and system design. Additionally, to support testing, Contractor provides a tailored training approach and plan based on the scope of your project and your designated users and user groups. This is outlined in Section "13. Training Services" of this SOW. The SSP stage 6.0 Risk Assessment and stage 7.0 POAMs will be completed during this phase. Additionally, the SSP ATO process will be defined during this stage.

All of the associated progress and risks for these stages will be reported on a regular cadence via project reports and meetings.

Implementation Phase - Contractor will implement the solution in accordance with the State approved systems configuration plan that will be based on the discovery and business analysis sessions. system acceptance will occur when MDOS provides Contractor with written acceptance of the product after System Configuration and System Testing are completed. All milestones that require acceptance by the State will be tracked accordingly.

Project Monitoring and Control Phase - Contractor will leverage project reports and meetings to track the project status, progress, blockers, milestones and any other critical insights as outlined in section "22. Project Control & Reports".

Project Closeout Phase - Post acceptance of the system, Contractor will leverage the agreed upon project plan to coordinate a system go-live and finish executing the documented transition plan accordingly. Additionally, mutually agreed upon SSP POAMs between Contractor and the State will be completed.

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, determine lifecycle management tool, determine team norms, initial SUITE project tailoring	Refer to Milestones/Payment in Schedule B.
Requirements and Design Validation	Discovery and Validation sessions, Requirement Validation Document,	Refer to Milestones/Payment in Schedule B

	<p>Network Diagram Design (Test and Prod), Role-Based Security Matrix, Design Document, Implementation Document, Detailed Requirements, EASA development & approval (2-3 weeks) , EASA Approval</p> <p>SSP Stages 1.0-5.0</p>	
Provision environments	Validate Test and Production environments	Refer to Milestones/Payment in Schedule B
Installation and Configuration of software	<p>Solution and Testing Documents Solution and Testing Document, Technical Baseline document with final configurations</p> <p>SSP Stage 6.0 Risk Assessment SSP Stage 7.0 POAMs</p>	Refer to Milestones/Payment in Schedule B
Testing, User Acceptance Testing and Issue Resolution	<p>Test Plan, Test Scenarios, Requirements traceability matrix, Test Results Report, Training Documentation & User Manuals, Product stabilization, SSP ATO SSP Authority to Operate</p>	Refer to Milestones/Payment in Schedule B
Training Activities	Training will be delivered according to the agreed training plan	Refer to Milestones/Payment in Schedule B
Implementation and Go Live	Implementation Plan, Final Test Results Report, Final Training Documentation, Final Acceptance	Refer to Milestones/Payment in Schedule B
Post Production Warranty	Complete SSP POAMs. Included in the cost of solution.	Refer to Milestones/Payment in Schedule B

Post Implementation and Production Support Services	Ongoing after Final Acceptance. Solution configuration adjustment as needed Complete SSP POAMS	Refer to Milestones/Payment in Schedule B
---	--	--

24. ADDITIONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE A – TABLE 1 – BUSINESS SPECIFICATION WORKSHEET

Contractors must meet each business Specification on how they will meet the requirements in the document provided. Contractor must not alter the document.

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

Column A: Business Specification number.

Column B: Business Specification description.

NOTE: Configuration is referred to as a change to the solution that must be completed by the awarded Contractor prior to Go-Live but allows an IT or non-IT end user to maintain or modify thereafter (i.e. no source code or structural data model changes occurring).

Customization is referred to a modification to the solution's underlying source code, which can be completed as part of the initial implementation. All configuration changes or customization modifications made during the term of the awarded contract must be forward-compatible with future releases and be fully supported by the awarded Contractor without additional costs.

Contractor shall understand that customizations (i.e. changes made to the underlying source code of the solution) may not be considered and may impact the evaluation of the Contractor's proposal.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	REQUIREMENTS <u>SECTION 2:</u> CASE MANAGEMENT SYSTEM (Opening, Type, Assignment, etc.)	
1.0	The solution must support a minimum of 100 data fields across various tabs for each case. The names of the fields and content of the fields (e.g. text, numbers, date, IP address) should be customizable to fit investigative needs.	Contractor will provide out-of-the-box capabilities to customize current field labels or create new fields based on case template requirements. Contractor will support over 100 data fields across various tabs for each case
2.0	The solution must include a character-limited field that allows the storage of only the first six and last four digits of a credit card number.	Contractor will configure these fields within the system.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
3.0	The solution must allow case fields the ability to be cross-referenced by other cases and linked to other cases, as needed.	Cases in Contractor solution are given unique case numbers that can be linked and referenced in other cases, investigations, or reports
4.0	The solution must have a case details section, a case summary section, and a case notes section. These sections/fields must not be character limited. The fields should include text formatting options (e.g. bullets, bold, spell check).	Contractor's robust case template and dynamic form editor allow for the configuration of the information you want to collect for cases. A case details, summary and notes section can easily be supported without character limits and included text formatting options.
5.0	The solution must allow the use of existing and future OIS case type options (MDOS configurable) selectable	Contractor's robust Case Template tool allows for the creation of case types and case type options to meet your current and future

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	at the time of case opening/assignment. (Exhibit 2, Process Flows)	workflows.
6.0	The solution must allow case type (e.g. vehicle fraud changed to ownership dispute) to be changed during investigation.	Contractor allows for case types to be updated during an investigation through our case template configuration feature.
7.0	The solution must allow case type data classification (e.g., confidential, restricted) level to restrict access to authorized users only.	The System contains robust User Access Management, Access Control, Data Classification, and User Role settings that can be used together to meet the needs for securely partitioning and managing access to data.
8.0	The solution must allow case priority level to be set by end users.	Contractor supports configurable case priority levels that can be restricted to specific end users.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
9.0	The solution must allow MDOS configurable categories for the purpose of identifying worksites (MDOS configurable list) upon case opening.	Contractor's dynamic form editor tools allow for configurable dropdown selection fields that can contain worksites and other customized lists. These lists can be embedded within reports as drop-down selection options.
10.0	The solution must have the ability to associate new and existing cases for enforcement of interrelated investigations (e.g., ability to cross-reference individuals involved in cases).	As data is entered into Contractors database, it is auto matched, deduplicated and linked to cases. Individuals and other entities can be linked automatically or manually to interrelated investigations.
11.0	The solution must allow for pop-up/auto-fill functionality with the ability for a user to select from a list after conducting a search (e.g. search items	The system begins searching for matches as you start typing into the search tool. Pop-up and auto-fill results will appear as

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	related to cases such as last name “Smith” would return all results with “Smith” in them, attachments associated with cases, including scannable/searchable documents) and choose to import specific data sets into the new case for the purpose of case linking.	matches are identified. Search results will identify all possible matches and multiple results with the same name. Standard search functions include phonetic, wildcard, area, translated, simple, full-text, partial-text, object type, Boolean, date-range, and geospatial searches.
12.0	The solution must allow electronic documents of multiple file types to be uploaded and associated with individual cases (e.g., excel, pdf, jpg, mp4, associated with single or multiple case numbers).	Any document and media that exists in electronic, digital image, audio and video format (Word, Excel, PDF, JPG, MP4, etc.) can be imported into Contractors database, in which case all text in the imported document or references to the imported file will be automatically

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		extracted and made available for searching. Media files can be viewed directly within the case and can also be downloaded for further analysis in other systems. Files and attachments can also be tagged, labeled, and easily connected to other entities and cases in the system as evidence or case related information.
13.0	The solution's default date for case opening should be the initial date the case is created in the solution. The solution must allow an override of date created by MDOS, if applicable.	The system's case template tool can be configured to auto-populate the current date upon case opening. The system's standard functionality provides the users to populate the current date in any date field with one click.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
14.0	The solution must allow MDOS configurable categories for the purpose of identifying worksites (MDOS configurable list) upon case opening.	Contractor's dynamic form editor tools allow for configurable dropdown selection fields that can contain worksites and other customized lists. These lists can be embedded within reports as drop-down selection options.
15.0	The solution must have the ability to associate new and existing cases for enforcement of interrelated investigations (e.g., ability to cross-reference individuals involved in cases).	As data is entered into Contractors database, it is auto matched, deduplicated and linked to cases. Individuals and other entities can be linked automatically or manually to interrelated investigations. Cases themselves can be linked to interrelated investigations.
16.0	The solution must allow for pop-up/auto-fill functionality with the ability	The system begins searching for matches as you start typing into the

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	for a user to select from a list after conducting a search (e.g. search items related to cases such as last name "Smith" would return all results with "Smith" in them, attachments associated with cases, including scannable/searchable documents) and choose to import specific data sets into the new case for the purpose of case linking.	search tool. Pop-up and auto-fill results will appear as matches are identified. Search results will identify all possible matches and multiple results with the same name. Standard search functions include phonetic, wildcard, area, translated, simple, full-text, partial-text, object type, Boolean, date-range, and geospatial searches.
17.0	The solution must allow electronic documents of multiple file types to be uploaded and associated with individual cases (e.g., excel, pdf, jpg, mp4, associated with single or multiple case numbers).	Any document and media that exists in electronic, digital image, audio, and video format (Word, Excel, PDF, JPG, MP4, etc.) can be imported into Contractors database, in which case all text in the imported

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		document or references to the imported file will be automatically extracted and made available for searching. Media files can be viewed directly within the case and can also be downloaded for further analysis in other systems. Files and attachments can also be tagged, labeled, and easily connected to other entities and cases in the system as evidence or case related information.
18.0	The solution's default date for case opening should be the initial date the case is created in the solution. The solution must allow an override of date created by MDOS, if applicable.	The system's case template tool can be configured to auto-populate the current date upon case opening. The system's standard functionality provides the users to

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		populate the current date in any date field with one click.
19.0	The solution must generate internal worker templates for individual cases based on case type when a case is initially saved (e.g., narrative report, coversheet, case supervision sheet). Templates must be auto-generated and associated to the case by default.	Custom internal form/report templates can be created using the dynamic forms editor tool. These forms/reports can be added as case actions through our case template tool. These case actions can be generated based off of specific case type being created and saved and be designed to be available and completed upon the completion of a parent case action.
20.0	Templates must be configurable by MDOS in the event associated templates change. The solution must allow authorized users to delete associated templates (must be	Contractor's solution was designed knowing that law enforcement agencies and departments have to adhere to different policies and workflows.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	configurable by MDOS, including ability to undo or correct a deletion).	The system is highly configurable and enables you to make simple changes as your policies and requirements change.
21.0	The solution must allow auto-save options (e.g., by field or otherwise determined by MDOS) for the purpose of reduction in loss of work (e.g., “save as you go process” to avoid data loss).	Contractor will provide this capability as part of its standard offering.
22.0	The solution must allow the ability to assign and reassign cases. This functionality must be role-based. Users must be able to self-assign cases. See Exhibit 2, Process Flows.	Contractor cannot restrict the ability to assign and self-assign cases by user type for our standard subscription users. Contractor does meet this requirement by allowing users to self-assign and

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		assign cases, Additionally, view only subscriptions and view only users can be restricted to just view cases and not assign or self-assign.
23.0	The solution must provide case-type specific data entry forms for multiple case types. (e.g., certain case types require different data collection fields than others.)	Custom workflows can be added to specific case types via the system's case template tool. The tool allows for reports, forms, and other case actions to be added to case types in any order that meets your requirements.
24.0	The solution must allow a user to change the case type and be alerted that other data entry fields are now required (based on new case type).	Custom workflows can be added to specific case types via the system's case template tool. When a case is updated with a different case type, those case type case actions will be generated, and users can be

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		notified of the case actions.
25.0	The solution must allow a case type to be changed during a case lifecycle without the loss of previously gathered case details and attachments.	The system allows for case types to be modified during a case lifecycle, while retaining any documents, forms and data information that has been linked to the case.
26.0	The solution must provide a “notes” functionality as part of the application for staff notes and comments.	Contractor includes a “Case Notes” feature that allows for the capture of notes for each case.
27.0	The solution must provide functionality to copy existing case details to a newly created case and retain/track the linkage between the individual cases.	Case reports, attachments and information from an existing case can be linked to a newly created case or an existing case. Existing and subsequent added information to either case will be linked and tracked by both cases.
28.0	The solution must allow for the use of existing case type and case disposition	The system comes with built-in case types and case disposition

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	codes and provide MDOS the ability to create new case type and case disposition codes.	codes, as well as the ability to add custom case types and case disposition codes.
29.0	The solution must allow end users with designated access the ability to cancel and delete cases.	Contractor's admin features allow permitted users with editor permissions the ability to delete existing cases.
	OPTIONAL REQUIREMENTS <u>SECTION 2</u> CASE MANAGEMENT SYSTEM (Opening, Type, Assignment, etc.)	
30.0	The solution should allow for a "bookmark" functionality that allows users to "pick up where they left off" in the system.	The system provides users with the capability to mark cases as a "favorite" providing you with the ability to quickly access cases marked as a "favorite".

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		<p>Additionally, the system's "My Workbox" and "My Open Cases" report that automatically provides you with quick and instant access to work and cases that are in-flight.</p>
	REQUIREMENTS <u>SECTION 3:</u> Searching, Sorting, and Prioritizing	
31.0	The solution must support search functionality on mobile devices.	Contractor will provide search capabilities on the mobile application.
32.0	The solution must provide search functionality for all data fields that includes wild card or partial match search options.	Standard search functions include phonetic, wildcard, area, translated, simple, full-text, partial-text, object type, Boolean, date-range, and

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		geospatial searches. All data in the system is made searchable through multiple technologies and search logics to include optical character recognition, Regex and Elasticsearch.
33.0	The solution must allow for restriction of search results display based on case data classification level and user role.	Contractor's access controls will allow search results to be visible based on user permission level and the classification level of the data being searched.
34.0	The content of all uploaded documents must be searchable.	As documents are uploaded into Contractors database, its content becomes searchable through multiple technologies and search logics to include optical character recognition, Regex and Elasticsearch.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
35.0	The solution must provide features for MDOS staff to sort search results (e.g., by date, user, case #, priority).	Search results in Contractors solution are sortable with a filter tool that allows you to filter results by document, entity, investigation/case, request, priority tags and a date range.
36.0	The solution must provide a save option for search criteria.	Any search may be saved for repeat use. Anytime new data that matches one of your saved searches is added to or updated in the system, you will automatically receive a notification
37.0	The solution must provide the ability to export search results.	Search results in Contractors solution can be exported as data in a CSV spreadsheet, PDFs, and combined zipped PDF files
38.0	The solution must provide the ability to track case related deadlines for case owners and managers. MDOS to have	Saved search reports can be designed to track case due- dates, deadlines, and other pertinent case

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	the ability to adjust deadlines and alerts as needed (e.g., case load and priorities).	action dates. Case owners and Managers will have the ability to modify dates and the types of alerts that are triggered.
39.0	The solution must provide search functionality for documents stored within the solution (e.g., searchable pdfs).	Documents stored within Contractors solution (e.g., PDFs, CSVs, Word documents) becomes searchable through multiple technologies and search logics to include optical character recognition, Regex and Elasticsearch.
	REQUIREMENTS <u>SECTION 4:</u> REPORTING AND PRINTING	
40.0	The solution must provide a reporting feature. The solution must support all	Contractor will include a relational data warehouse

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	reports based on data fields within the solution.	that can support the use of Contractor's Solution included Business Intelligence tools. These tools will allow Michigan OIS to measure and understand their data as needed to produce the analysis and statistics that matter most to them.
41.0	The solution must support 50 canned reports upon Go Live (e.g., biweekly, monthly, warrant request, branch incident, audit, open/closed, new case, evidence inventory log, chain-of-custody).	During system configuration, the system can be set-up to support 50 canned reports and others.
42.0	The solution must support Ad-hoc reporting that allows MDOS to generate a report based on data fields within the solution.	Contractor will include a relational data warehouse that can support the use of the Contractor. included Business

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		Intelligence tools that can provide ad-hoc reporting based on data fields.
43.0	The solution must support Ad-hoc exports on a scheduled basis as determined by MDOS.	User generated exports through our advanced search tool can be created and saved and designed to run on a scheduled basis.
44.0	The solution must provide viewable and/or printable case reporting functionality using MDOS configurable filtering and sorting features.	User generated exports through our advanced search tool can be sortable through many filters and sorting features. These results are viewable and printable.
45.0	The solution must provide the reports in a variety of file types (e.g., PDF, Excel, Word).	The system provides report export capabilities in PDF and Excel CSV format. These exports can also be emailed to external users directly from the system.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
46.0	The solution must allow for automated reporting (based on MDOS configurable criteria) to be sent at intervals determined by MDOS.	Contractor's reporting features can be configured to be automated based on your requirements.
47.0	The solution must allow for reports to display to which work sections/units the end users belong.	Contractor's access control features allow for users to be tagged to specific groups/units allowing for the relevant reports to be ran.
48.0	The solution must allow for printing of all cases (e.g., summary reports, narrative reports, external documents).	The system provides the ability to download cases as PDFs and then print directly from your workstation.
49.0	The solution must allow users to modify narrative sections and fields within a report (e.g., investigative report).	Contractor's robust dynamic forms editor tool allows for reports to be customized to meet your requirements.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		Narrative sections and fields can be designed to be modified or restricted based on your needs.
	REQUIREMENTS <u>SECTION 5:</u> ALERTS, DASHBOARD, METRICS, TRACKING	
50.0	The solution must provide dashboard functionality based on user role. See Exhibit 3, Dashboard Example.	Contractor will provide dashboards configurable to each user.
51.0	The solution must provide alert functionality using MDOS configurable triggers (e.g., new case, case assigned, case canceled, case closed) for notification based on user role (e.g., case owner, manager, executive).	Contractor's advanced search feature allows for searches with defined perimeters to be saved and ran continuously. Whenever new data matches a saved search it is added to or updated in the system, notifications can

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		then be automatically sent out to specific users based on their role.
52.0	The solution must provide alerts both within the solution and external e-mail notifications for case deadlines.	Contractor's case workflow features and business process engine can be configured to provide alerts internally and externally.
53.0	The solution must provide reporting metrics for real time case status (e.g., open, closed, warrant).	Contractor's advanced search tool provides a report for real time case status for all cases. This report can be saved and presented on users dashboard.
	REQUIREMENTS <u>SECTION 6:</u> APPLICATION IDENTIFICATION/USER ROLE	
54.0	The solution must allow for role-based functionality (e.g., agency/analyst,	The system contains robust User Access Management, Access

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	administrative support, manager, executive, system administrator).	Control, Data Classification, and User Role settings that can be used together to meet the needs for securely partitioning and managing access to data. These settings can be configured to limit, restrict, or deny access to data or actions based on a variety of criteria such as case types, incident types, user groups/teams, individual users, and other defined data classification criteria.
55.0	The solution must restrict the closing and reopening of cases to specific user roles, as configured by MDOS.	Contractor's access controls can restrict specific users from being able to open and close cases.
56.0	The solution must restrict the cancelation of cases to a specific role, as configured by MDOS. The solution	Contractor's access controls can restrict specific users from being able to cancel and delete cases. A custom deletion/cancellation

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	must require a cancelation reason with comments (unlimited character limit).	reason field can be added to cases. This custom field is included in the cost via design during joint application development sessions and then configured accordingly at no additional cost to the State.
57.0	The solution must allow for an end user profile that includes work unit and role in the system.	Contractor's Solution comes with robust user access controls and organization functionality that is all viewable from within the system. In their settings, a user can see their role and groups/units that they are a part of.
58.0	The solution must allow for unique identifiers for different contact types that contact OIS (e.g., complainant, investigator, suspect, witness).	Contractor's dynamic form editor can be used to create contact type fields for ingesting contact information types.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
59.0	The solution must allow for unique identifiers for different property types (e.g., stolen property, evidence, other).	Entities in Contractor solution (persons, places or things) can be referenced and saved in Contractors solution.
60.0	The solution must enforce completion requirements (e.g., tasks, reviews, other requirements) prior to allowing case closure (as determined by designated approval role) to occur.	The system allows for case types and case workflows to be configured with required case actions that must be completed prior to case closure.
61.0	The solution must provide an MDOS-configurable workflow for notifications and reminders based on user role (e.g., dashboard for notifications of outstanding tasks) and duration (e.g., 15-day, 30-day). See Exhibit 2, Process Flows.	The system allows for case types and case workflows to be configured with case action notifications and reminders to automatically be triggered.
62.0	The solution must restrict the visibility of cases based on case type and user	The system's access control features allow access to cases to

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	access level and be configurable by MDOS.	be restricted, blocked, or limited based on defined user types.
63.0	The solution must have the ability to apply a security level to individual cases for access management (e.g., confidential). Solution must include hiding confidential cases from search results for end users that do not have designated access.	Authorized users can restrict cases to specific groups that will only have access to the case. This includes hiding the case from search results from other user groups. This can be done through the system's access control features.
	REQUIREMENTS <u>SECTION 7:</u> TEMPLATES	

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
64.0	The solution must provide 25 templates as part of Go Live (e.g., letters, chain of custody forms, evidence list).	During project set-up and configuration, Contractor's dynamic form editor and case template tool will be used to set-up all the templates that are required for MDOS.
65.0	The solution must allow end users the ability to delete an attachment from within specific case files prior to submitting the case for management approval.	Contractor's case process flow features allows for users to delete attachments within cases, prior to being submitted for approval.
66.0	The solution must allow end users with designated access and approval authority to delete attachments from the solution (to ensure deleting attachment	Contractor users can be designated with view only rights, allowing for only authorized users the ability to delete attachment from the solution.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	is not impacting other existing case files).	
	REQUIREMENTS <u>SECTION 8:</u> EVIDENCE COLLECTION (BARCODE/SCANNER)	
67.0	The solution must provide an evidence collection module for scanning, logging, and tracking evidence received.	Contractor includes a flexible and configurable evidence management module that supports evidence collection processes such as scanning, logging, inventory, chain of custody and location tracking. This module is supported on Contractor's iOS and Android mobile application.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
68.0	The solution must support “chain-of-custody” functionality for evidence collected (e.g., log for date, time, location, name of end user collecting evidence, description, who is currently in possession of evidence).	The Contractor evidence management module supports various chain-of-custody features to include logging, date tracking, location, name, collection information, witnessing, inventory, location, and more.
69.0	The solution must include printing a property label that includes a unique barcode and MDOS configurable fields for details (e.g., date, obtained from, description, bar code).	The parties agree that Contractor will create a new field on the label that provides a number designating whether it is the 1st, 2nd, 3rd, etc. evidence item in a case, to meet this requirement, subject to Final Acceptance by the State.
70.0	The solution must provide barcode and qr code scanning capabilities for the purpose of scanning in labeled evidence by end users.	The Contractor solution supports this scanning requirement with commercial-off-the-shelf functionality.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
71.0	The solution must provide the ability to link barcoded/scanned evidence to specific cases (or multiple cases, as needed).	Contractor is uniquely designed to support the linking of all data in the system to other data and system features. Evidence can be linked to multiple cases, reports, investigations, etc. throughout the application.
72.0	The solution must provide a corresponding receipt for the property label.	System meets requirements.
	REQUIREMENTS <u>SECTION – 10</u> REDACTION	
73.0	The solution must allow an ability to manually redact information.	Contractor will provide the ability to redact select information when exporting and emailing cases, reports, and other content from the system. This redaction

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		interface is accomplished through check boxes that allow you to select and choose what information you would like exported and/or emailed. Additionally, records managers can edit finalized documents and entities as a means of permanently redacting sensitive information.
74.0	The solution must allow MDOS users to configure and edit, without vendor action, a list of redaction reasons (e.g., statutory citations).	Contractor provides retention tools that allow for these lists to be generated.
75.0	The solution must retain the original unredacted version of any record and create and retain a separate redacted copy of the record.	The system allows for the unredacted versions to be maintained and retained in the solution. Separated redacted

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		copies can be attached and referenced in cases.
76.0	The solution must require MDOS users to select a redaction reason (e.g., statutory citation) for any redaction made and tie it to the redaction and add comments if desired.	System meets requirements. Be tagged to cases explaining why a document is redacted.
77.0	The solution must allow an ability to cite specific statute, and additional comments if required, to tie to a redacted item as part of redaction functionality.	Contractor's solution provides this as part of its standard functionality.
	REQUIREMENTS <u>SECTION - 11</u> SECURITY	

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
78.0	The solution must allow device (mobile and non-mobile) access to be restricted to trusted state-owned devices only.	Access to the Contractor application can be restricted based on IP address.
79.0	The solution must allow for the creation of multiple user roles with varied (configurable) system access and capabilities.	The System contains robust User Access Management, Access Control, Data Classification, and User Role settings that can be used together to meet the needs for securely partitioning and managing access to data. These settings can be configured to limit, restrict, or deny access to data based on a variety of criteria such as case types, incident types, user groups/teams, individual users, and other defined data classification criteria

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
80.0	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.	Administrator roles can be given configurable and custom controls over what they need access to.
81.0	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.	Customers authenticate to the Contractor application using SSO, which is managed by the customer. Customers are allowed to limit access to data through role-based access controls.
82.0	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.	Contractor will configure this role to meet your specific requirements.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
83.0	<p>System Roles:</p> <p>A. MDOS Security Administrator</p> <ul style="list-style-type: none"> • Able to add/remove users • Able to change user roles • Cannot do anything else in the application (ex: cannot process filings) • Security reports <p>B. MDOS Administrator</p> <ul style="list-style-type: none"> • Able to edit templates & some settings • Able to edit user role functions • Cannot do anything else in the application (ex: cannot process filings) • Security Reports <p>C. No “All Powerful” system admin user role</p>	Contractor will configure this role to meet your specific requirements.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
84.0	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).	Contractor will collaboratively work with MDOS to assist with the SSP process inline with the SUITE process.
85.0	Document the maintenance plan including the request, approval, and record keeping methodology (MA-02). Please indicate whether or not access to production data is required.	Tickets for bugs or system issues can be submitted directly from within the system, and communication on the ticket specific issues are through email and phone call communications. Release notes are included in the system and are provided in advance. Any required downtime is notified in advance.
86.0	The solution must include contiguous annual SOC 2 Type II compliance for	Contractor will maintain an annual SOC 2 Type II for Security and

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	the five AICPA Trust Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.	Confidentiality. Availability, Processing and Privacy can be pursued if required.
87.0	Vendor to provide ongoing annual contiguous SOC 2 Type II report for the Application and ongoing annual contiguous SOC 2 Type II report for Hosting for the five AICPA Trust Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.	Contractor will maintain an annual SOC 2 Type II for Security and Confidentiality. Availability, Processing and Privacy can be pursued if required.
88.0	Provide AICPA Complementary User Entity controls in place by vendor for any subservice organizations used (AWS, Azure, etc.) as defined in the SOC report.	Contractor provided to MDOS
89.0	Provide a list of all subservice organizations and their associated products that are used to host,	Contractor provided to MDOS

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	maintain, provide additional services, or build the application.	
90.0	If externally hosted, the data (including test, production, backup/recovery data) must be hosted only in the United States.	All data will be hosted in the United States.
91.0	The information system automatically disables inactive user accounts after 60 days and system accounts after 365 days.	Customers authenticate to the Contractor application using SSO, which is managed by the customer. SSO is required to disable user accounts after a defined period of time.
92.0	No temporary, emergency, or group accounts.	Customers authenticate to the Contractor application using SSO, which is managed by the customer.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
93.0	If externally hosted, the data must be hosted in a FedRAMP moderate authorized environment.	Contractor is hosted on Microsoft Azure Government Cloud which is FedRAMP High. Contractor solution is hosted on Microsoft Azure Government Cloud which is FedRAMP High
94.0	If externally hosted, the data should be stored in the government cloud (as opposed to commercial cloud) if one exists.	Contractor is hosted on Microsoft Azure Government Cloud which is FedRAMP High.
95.0	The information system automatically documents account creation, modification, disabling, and removal actions.	The system has extensive internal monitoring capabilities that track various actions.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
96.0	The information system enforces a limit of three invalid logon attempts within a defined time period during a user session upon which the account/node is automatically locked for a minimum period of 30 minutes or until released by an administrator.	Customers authenticate to the Contractor application using SSO, which is managed by the customer.
97.0	The information system displays a customizable message or warning banner before granting access to the system.	Customer administrators can set login messages that will display to all users.
98.0	The information system initiates a session lock after a configured number of minutes of inactivity. The information system session lock, when activated, places a publicly viewable pattern onto the associated display, concealing what was previously visible on the screen.	Users are logged out based on configuration.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
99.0	The information system must terminate a user's session after a defined period of inactivity.	Customers authenticate to the Contractor application using SSO, which allows customers to configure session locks. This is configurable through Keycloak. The Solution is capable of meeting this requirement without relying on the SSO provider.
100.0	The information system must be able to generate an audit of the following events: <ul style="list-style-type: none"> • User account management activities: Creation, Modification, or deletion of accounts. • Use of Administrator privileges. • End user viewing events (e.g., looking at a case). 	Customers authenticate to the application using SSO. Customers identity management solution logs user account management activities. The Contractor application logs end user events. The Solution is capable of meeting this requirement without relying on the SSO provider.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
101.0	<p>The information system generates audit records containing:</p> <ul style="list-style-type: none"> • 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. • The source of the event. • The destination of the event. • The outcome of the event. • Where IP address is stored/located/identified • The solution must track and generate audit log reports that show who is accessing and viewing cases, case-related documents, and viewing other information system data. 	Contractor's robust audit tools can generate audit records for the desired information.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	The identity of any individuals or subjects associated with the event.	
102.0	<p>The following events shall be logged:</p> <ol style="list-style-type: none"> 1. Successful and unsuccessful system log-on attempts. 2. Successful and unsuccessful attempts to use: <ol style="list-style-type: none"> a. access permission on a user account, file, directory or other system resource; b. create permission on a user account, file, directory or other system resource; c. write permission on a user account, file, directory or other system resource; d. delete permission on a user account, file, directory or other system resource; e. change permission on a user account, file, directory or other system resource. 	<p>Customers authenticate to the Kasware application using SSO. Customers identity management solution logs user account management activities. The Contractor application logs end user events.</p>

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	<p>3. Successful and unsuccessful attempts to change account passwords.</p> <p>4. Successful and unsuccessful actions by privileged accounts (e.g., root, Oracle, DBA, admin)</p> <p>5. Successful and unsuccessful attempts for users to:</p> <ul style="list-style-type: none"> a. access the audit log file; b. modify the audit log file; c. destroy the audit log file. <p>These events must be available for review through audit log reports.</p>	
103.0	Sufficient audit storage capacity to support ongoing operations and rollback of the system. System sends an audit storage alert when capacity is getting low.	The system provides no limits on audit storage capacity.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
104.0	The solution must automatically generate and send the audit logs as specified by MDOS on a weekly basis.	Contractor Solution provides significant user logging capabilities and is accessible by administrators. Logs can be exported from the system as needed.
105.0	Information system must use internal system clocks mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and maintains time synchronization within 20 milliseconds of reference clocks.	The system can be configured to be mapped to your desired time zone. It will maintain the desired time synchronization.
106.0	The information system and operating system, for password-based authentication: <ul style="list-style-type: none"> Stores and transmits only cryptographically protected passwords. 	Contractor will utilize Redhat Keycloak to manage authenticators and can be configured to the needs of the customer. Otherwise Keycloak can be set up to

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	<ul style="list-style-type: none"> Enforces password minimum and maximum lifetime restrictions. Prohibits password reuse for a defined set of generations. <p>Supports State of Michigan password complexity requirements.</p>	authenticate against the customer's SSO.
107.0	The solution inputs and outputs must meet SOM standards for database security (e.g., not create, use, or rely on Microsoft Access databases or similar database software).	Contractor inputs and outputs meet SOM standards for database security.
108.0	The vendor must provide a description of the functional properties of the security controls to be employed. Provide design and implementation information for the security controls and application.	Contractor will provide Security Policies upon request.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
109.0	The vendor must provide a comprehensive system configuration manual and technical baseline.	Contractor Provided document.
110.0	The system shall be configured to provide only essential capabilities and restrict the use of specified functions, ports, protocols, and/or services.	The system can be configured to only meet your needs, with other features and capabilities turned off.
111.0	Provide evidence of secure coding & use of security engineering principles.	Contractor will provide this.
112.0	Define a written flaw remediation process that includes approval of the change, verification that the change was implemented correctly, and a tracking process.	Contractor will provide this.
113.0	A list of protections in place that prevent unauthorized and unintended	Contractor Solution is hosted on Microsoft Azure Government (CJIS compliant) Cloud with all customer

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	information transfer via shared system resources.	data logically separated. Contractor uses tenant ID and access controls to logically segregate data.
114.0	List the technologies in place to prevent DDOS attacks.	Contractor will use Microsoft Azure cloud services to provide increased capacity and bandwidth in case of a DDoS attack.
115.0	List the types of managed interfaces (firewalls, routers, subnets, etc.) that protect the boundary of the application.	Contractor utilizes Microsoft Azure firewall.
116.0	Encrypts all data in flight using FIPS 140-2 certified and a cypher key strength of at least 128 bit AES and TLS 1.2, HTTPS or higher.	Data in Contractors Solution is encrypted in flight to these standards.
117.0	Encrypts all data at rest using a symmetric cypher that is FIPS 197 certified (AES) and at least 256-bit strength.	Data at rest is encrypted on Microsoft Azure Cloud using 256 bit AES encryption which is FIPS 140-2 compliant.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
118.0	Document how encryption keys are managed and protected.	Contractor utilizes Microsoft Azure Key Vault to manage encryption keys
119.0	The information system must conform to MDOS and/or State of Michigan's established record retention policies and schedules. The solution must be able to be programmed and configured by the State to retain and automatically purge records based on retention schedules as defined by the State. The record retention policy must be based on case closure date.	Contractor's robust data retention tools can be configured to meet the States or MDOS' requirements.
120.0	The vulnerability remediation timeline must be in alignment with the remediation requirements defined within State of Michigan policy, standard, and procedure.	Contractor remediates high risk vulnerabilities within 30 days; moderate risk vulnerabilities within 90 days; an low risk vulnerabilities within 180 days from date of discovery.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
121.0	MDOS should be able to receive a copy of the data for records retention storage on premise on request.	Client may request copy of data stored in the Contractor application for an additional fee
122.0	Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.	Current Capability
123.0	Information system must detect attacks and indicators of potential attacks in accordance with Michigan Security Operations Center (MiSOC) monitoring standards and procedures.	Contractor monitoring includes Microsoft Azure, Crowdstrike Falcon Complete, and a SIEM.
124.0	Employs integrity verification tools to detect unauthorized changes to software, firmware, and information.	Contractor relies on Microsoft Azure to prevent unauthorized changes to software, firmware, and information.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
125.0	The information system checks the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	Contractor implements a variety of checks to ensure inputs are complete and accurate. Additionally, customers can configure inputs and their individual requirements.
126.0	Version control software must be used.	Current Capability
127.0	Development, Testing, and Production environments must be separated.	Contractor will utilize various environments to allow for this.
128.0	Hosted Services must be scanned for vulnerabilities every month. A report of the scan results and the name of the tool used should be provided to MDOS each month.	Contractor will negotiate what reports and desired scans will be needed each month
129.0	Vulnerability scan report and results must meet SOM SADLC requirements. A report of the scan results and the	Contractor will provide annual SOC 2 Type 2 which provides audit of vulnerability scan reports and annual penetration test.

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
	name of the tool used should be provided to MDOS each month.	Additional requirements will likely include additional service fees.
130.0	The vulnerability scanning tool must be updated before each scan.	Contractor will fulfill this requirement.
131.0	Michigan Cyber Security must be permitted to scan the application for vulnerabilities.	Contractor will follow strict security protocols. All data in the Contractor platform is encrypted using the latest encryption standards, both at rest and in transit. Contractor regularly undergoes penetration testing to ensure that you're protected against the latest threat vectors. We regularly leverage independent audits and are compliant with SOC 2 Type 1 and SOC 2 Type 2 and CJIS. Contractor will provide a copy of the

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		annual penetration test upon request.
132.0	Evidence that security patches are up to date must be provided to MDOS.	Contractor must provide this evidence.
133.0	Obtain public key certificates from an approved service provider.	Contractor will fulfill this requirement.
134.0	Application must maintain a separate execution domain for each executing process.	Contractor will employ process isolation technologies.
135.0	Provides release notes on maintenance activity, patching cycles and system updates to MDOS.	Contractor will provide this.
136.0	Nonlocal maintenance activities may only be done through a SOM VPN.	Contractors solution is hosted in Microsoft Azure shared cloud. SOM VPN is not used because Contractor solution is not hosted

A	B	D
Business Specification Number	Business Specification	Contractor must explain how they will deliver the business Specification. Explain the details of any configuration/customization and the impacted risk that may be caused if configured or customized to meet the business specification.
		by SOM

SCHEDULE B - PRICING

Contractor must also provide tiered pricing for hosting to accommodate future growth or reductions.

Table A - Subscription License Fee

Subscription Based - Product Name	Annual License Subscription Fee (Price per user)	Annual Tiered Pricing	Monthly Tiered Pricing	Annual Enterprise Licensing – Unlimited Number of Users
Kaseware Government Subscription	\$1,200	50-99 users = \$1,080 100-249 users = \$960 More than 250 users = \$840	\$100 per user per month For 50-99 users, \$90 per user per month For 100-249 users, \$80 per user per month More than 250 users, \$70 per user per month	Not Available

Licensing and Hosting costs will be paid after installation, configuration, and State testing and acceptance of the Solution. Hosting costs are included in the subscription price.

1. Implementation Fees. All costs associated with Implementation Services are included below (e.g. configuration, customization, migration, integration, testing, etc.) (the "Implementation Fees"). All costs are firm fixed.

All payments under the Milestone Table will be payable after Acceptance of the applicable Milestone Deliverable. Contractor to implement solution within 12 months of contract execution, subject to MDOS approval of final implementation schedule (allows considerations for integrations with CARS, MILogin, and staff availability).

Implementation		
Implementation Stages	Associated Milestone Deliverable(s)	One- time Cost
Project Planning	Project Kickoff, determine lifecycle management tool, determine team norms, initial SUITE project tailoring	\$22,200.00
Requirements / Design Validation	Discovery and Validation sessions, Requirement Validation Document, Network Diagram Design (Test and Production), Role-Based Security Matrix, Design Document, Implementation Document, Detailed Requirements, EASA development & approval (2-3 weeks) , EASA Approval SSP Stages 1.0-5.0	\$39,600.00
Provision Environments	Validate Test and Production environments	\$22,200.00
Installation & Configuration	Solution and Testing Documents Solution and Testing Document, Technical Baseline document with final configurations SSP Stage 6.0 Risk Assessment SSP Stage 7.0 POAMs	\$22,200.00
Testing	Test Plan, Test Scenarios, Requirements traceability matrix, Test Results Report, Training Documentation & User Manuals, Product stabilization, SSP ATO	\$58,800.00
Training (2)	Two (2) on-site training sessions are included as part of the implementation fee. Each session consists of 2 on-site days of training with a contractor technical trainer.	\$0.00
Implementation & Go Live	Implementation Plan, Final Test Results Report, Final Training Documentation, Final Acceptance	\$186,000.00
Post-Production Warranty	Complete SSP POAMs. Included in the cost of Solution	\$0.00
Total		\$351,000.00
After Acceptance of an implementation stage the invoice will be paid in accordance with Sec 13 of the Software Contract Terms		

Ongoing Annual	
Ongoing Annual	Annual Cost
Annual Subscription (based 50 users @\$1,080 each)	\$54,000.00
Annual Production Support	\$15,000.00
Total	\$69,000.00
Ongoing costs begin after the Warranty Period.	

2. Rate Card for Ancillary Professional Services.

Resource	On-Site Hourly Rate	On-Shore and Off- Site Hourly Rate
Custom Development*	\$300 per hour	\$200 per hour
Non-Technical Support**	\$250 per hour	\$150 per hour

*Custom Development - Hourly rate for custom development work. Estimates would be provided prior to work beginning. Custom development only applies to enhancements created pursuant to future Statement of Works. There will be no additional cost incurred for enhancements performed pursuant to the current Statement of Work.

**Non-Technical Support (e.g., on-site support) - Hourly rate for training and configuration work that falls out of scope for what is considered “normal support”, as set forth in Schedule D – SLA, Section 3.1. Estimates would be provided prior to work beginning.

3. Open Source or Third Party Products

The Contractor must identify any open source or third-party products that include a separate licensing fee and will be used in connection with the proposed Solution.

Product	Price
n/a	n/a

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 notice to the State's Contract Administrator with the reduced prices within fifteen(15) Business Days of the reduction taking effect.

Travel and Expenses

The State does not pay for overtime or travel expenses.

SCHEDULE C - INSURANCE REQUIREMENTS

1. **General Requirements.** Contractor, at its sole expense, must maintain the insurance coverage as specified herein for the duration of the Term. Minimum limits may be satisfied by any combination of primary liability, umbrella or excess liability, and self-insurance coverage. To the extent damages are covered by any required insurance, Contractor waives all rights against the State for such damages. Failure to maintain required insurance does not limit this waiver.
2. **Qualification of Insurers.** Except for self-insured coverage, all policies must be written by an insurer with an A.M. Best rating of A- VII or higher unless otherwise approved by DTMB Enterprise Risk Management.
3. **Primary and Non-Contributory Coverage.** All policies for which the State of Michigan is required to be named as an additional insured must be on a primary and non-contributory basis.
4. **Claims-Made Coverage.** If any required policies provide claims-made coverage, Contractor must:
 - a. Maintain coverage and provide evidence of coverage for at least 3 years after the later of the expiration or termination of the Contract or the completion of all its duties under the Contract;
 - b. Purchase extended reporting coverage for a minimum of 3 years after completion of work if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract.
5. **Proof of Insurance.**
 - a. Insurance certificates showing evidence of coverage as required herein must be submitted to DTMB-RiskManagement@michigan.gov within 10 days of the contract execution date.
 - b. Renewal insurance certificates must be provided on annual basis or as otherwise commensurate with the effective dates of coverage for any insurance required herein.
 - c. Insurance certificates must be in the form of a standard ACORD Insurance Certificate unless otherwise approved by DTMB Enterprise Risk Management.
 - d. All insurance certificates must clearly identify the Contract Number (e.g., notated under the Description of Operations on an ACORD form).
 - e. The State may require additional proofs of insurance or solvency, including but not limited to policy declarations, policy endorsements, policy schedules, self-insured certification/authorization, and balance sheets.

f. In the event any required coverage is cancelled or not renewed, Contractor must provide written notice to DTMB Enterprise Risk Management no later than 5 business days following such cancellation or nonrenewal.

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

7. Limits of Coverage & Specific Endorsements.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Personal & Advertising Injury \$2,000,000 Products/Completed Operations \$2,000,000 General Aggregate	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
Minimum Limits: \$1,000,000 Per Accident	Contractor must have their policy: (1) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds; and (2) include Hired and Non-Owned Automobile coverage.

Required Limits	Additional Requirements
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

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

SCHEDULE D – SERVICE LEVEL AGREEMENT

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

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

“Availability” has the meaning set forth in **Section** Error! Reference source not found..

“Availability Requirement” has the meaning set forth in **Section** Error! Reference source not found..

“Available” has the meaning set forth in **Section** Error! Reference source not found..

“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” has the meaning set forth in **Section 3.9**.

“Critical Service Error” has the meaning set forth in **Section 2.4**.

“Exceptions” has the meaning set forth in **Section 2.2**.

“High Service Error” has the meaning set forth in **Section 2.4**.

“Low Service Error” has the meaning set forth in **Section 2.4**.

“Medium Service Error” has the meaning set forth in **Section 2.4**.

“Resolve” has the meaning set forth in **Section 2.4**.

“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" has the meaning set forth in **Section 2.3**.

"Scheduled Uptime" means the total minutes in the Service Period.

"Service Availability Credits" has the meaning set forth in **Section Error!**
 Reference source not found..

"Service Error" means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

"Service Level Credits" has the meaning set forth in **Section 3.8**.

"Service Level Failure" means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

"Service Period" has the meaning set forth in **Section 2.1**.

"Software Support Services" has the meaning set forth in **Section 3**.

"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.

"Support Hours" means, Monday thru Friday, 8 a.m. – 5 p.m. EST

"Support Request" has the meaning set forth in **Section 3.5**.

"Support Service Level Requirements" has the meaning set forth in **Section 3.4**.

2. Service Availability and Service Available Credits.

2.1 Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a **"Service Period"**), at least 99.98% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the **"Availability Requirement"**). **"Available"** means 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. **"Availability"** has a correlative meaning. The Hosted Services and Software are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services and Software, in whole or in part. The Availability Requirement will be calculated for

the Service Period as follows: $(\text{Actual Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \div (\text{Scheduled Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \times 100 = \text{Availability}$.

2.2 Exceptions. No period of Hosted Services degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following ("**Exceptions**"):

- (a) Failures of the State's or its Authorized Users' internet connectivity;
- (b) Scheduled Downtime as set forth in **Section 2.3**.

2.3 Scheduled Downtime. Contractor must notify the State at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services or Software in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve extensions of Scheduled Downtime above five (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 two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

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

2.6 Remedies for Service Availability Failures.

(a) If the actual Availability of the Hosted Services and Software is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the fees payable for Hosted Services and Software provided during the Service Period ("**Service Availability Credits**"):

Availability	Credit of Fees
≥99.98%	None
<99.98% but ≥99.0%	15%
<99.0% but ≥95.0%	50%
<95.0%	100%

(b) Any Service Availability Credits due under this **Section 2.6** will be applied in accordance with payment terms of the Contract.

(c) If the actual Availability of the Hosted Services and Software is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

3. Support and Maintenance Services. Contractor will provide IT Environment Service and Software maintenance and support services (collectively, “**Software Support Services**”) in accordance with the provisions of this **Section Error! Reference source not found.** The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

3.1 Support Service Responsibilities. Contractor will:

(a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;

(b) provide unlimited telephone support Monday – Friday 8:00 am to 5:00 PM Eastern Standard Support Hours (Other),

(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 twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service 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, 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 or any Hosted Service 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 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 **Section 3.5 and 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 must provide all information to the State about modifications or upgrades to 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.

3.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 3.4 ("Support Service Level Requirements")**, and the Contract.

3.5 Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a **"Support Request"**). The State will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	<ul style="list-style-type: none"> • Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions.
High Service Error	<ul style="list-style-type: none"> • Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.

Support Request Classification	Description:
	Any Service Error Comprising or Causing any of the Following Events or Effects
Medium Service Error	<ul style="list-style-type: none"> IT Environment Services and Software is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work around.
Low Service Error	<ul style="list-style-type: none"> Request for assistance, information, or services that are routine in nature.

3.6 Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. **“Resolve”** (including **“Resolved”**, **“Resolution”** and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error. Service Level Credits are calculated based on the ongoing annual cost table located in Schedule B – Pricing:

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	One (1) hour	Three (3) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (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.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (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	One (1) hour	Four (4) hours	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for the first additional hour or portion thereof that the corresponding

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
			or portion thereof that the corresponding Service Error is not responded to within the required response time.	Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
Medium Service Error	Three (3) hours	Two (2) Business Days	N/A	N/A
Low Service Error	Three (3) hours	Five (5) Business Days	N/A	N/A

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 sixty (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. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 3.1 ("Service Level Credits")** in accordance with payment terms set forth in the Contract.

3.9 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) 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 five (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. 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 IT Environment 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 continental United States. The force majeure provisions of this Contract do not limit Contractor's obligations under this section.

4.1 Data Storage. Contractor will provide sufficient storage capacity to meet the needs of the State at no additional cost.

4.2 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 five (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.

4.3 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 one (1) Business Day of the State's request. Contractor will provide data restorations at its sole cost and expense.

4.4 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 one (1) hour , and a Recovery Time Objective (RTO) of four (4) hours (the “**DR Plan**”), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor’s current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule F**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 4**; and provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor’s receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

Korinne Condie – Chief Operating Officer - 720-597-0493

Sarah Crank – Director of Customer Operations – 307-223-6944

Liam Hollins – Technical Support Engineer – 720-292-8512

Louis Strube – Technical Project Coordinator – 540-246-8399

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 under this Contract.

“MOD” means moderate.

“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 Hosted Services who has sufficient knowledge of the security of the Hosted Services 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 Representatives 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/0,5552,7-358-82547_56579_56755---,00.html.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the contracted 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 Policy. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. 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 pursuant to **Section 15.1** of the Contract;

5.2 for Hosted Services provided by the Contractor, maintain either FedRAMP authorization or an annual contiguous 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. SOC 2 Type II audit reports on the Hosted Services must address all five trust principles of Security, Availability, Confidentiality, Processing Integrity, and Privacy. The Contractor must provide its SSAE 18 SOC 2 Type II audit report to the State within thirty (30) days of the Contractor's receipt of such report.

5.3 For the application provided by the Contractor, maintain a FedRAMP authorization or an annual contiguous 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. SOC 2 Type II audit reports on the Hosted Services must address all five trust principles of Security, Availability, Confidentiality, Processing Integrity, and Privacy. Contractor must provide copies of such audit reports covering controls on its own organization as well as controls on its subcontractor organizations, with the understanding that Contractor's June, 2024, SOC report will include all five trust control principles outlined above. Contractor must annually document how it meets each subcontractor organization's complementary user controls. The Contractor must provide its SSAE 18 SOC 2 Type II audit report to the State within thirty (30) days of the Contractor's receipt of such report.

5.4 ensure that the Software and State Data is securely hosted, supported, administered, accessed, and backed up in a data center(s) that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

5.5 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;

5.6 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, CJIS, SSA, HIPAA, FERPA and PCI requirements as applicable);

5.7 take all reasonable measures to:

- a. secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services 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 Services; (ii) State Data from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State Data;

5.8 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;

5.9 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;

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

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 five (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 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 Secure Web Application 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) – Scanning interactive 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 industry-standard application scanning tool, and provide the State with a vulnerabilities assessment after Contractor has completed such scan. These scans and assessments i) must be completed and provided to the State quarterly (dates to be provided by the State) and for each major release; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

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

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

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

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

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

- a. If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programming interface (API).
- b. Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must ensure the infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI or other 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. Media Sanitization

11.1 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 sign an affidavit of destruction if requested by the State.

11.2 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.

12. Nonexclusive Remedy for Security Breach.

12.1 Any failure of the Services to meet the 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 –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

SCHEDULE F – DISASTER RECOVERY PLAN

Policy Name: Kaseware Contingency Planning Policy

Policy # 6.0.0

Effective Date: 05/06/2021

REVISION HISTORY

Version	Date	Reviewer	Comments
1.0	4/12/2018	Nathan Burrows	Original Policy
1.1	3/22/2019	Nathan Burrows	Updated new office physical access system.
1.2	3/20/2020	Sarah Crank	Compiling all forms
2.0	6/2/2020	Nathan Burrows	Security Policy Manual update
2.1	8/24/2020	Nathan Burrows	update
3.0	5/6/2021	Scott Schons	Remove Disaster Recovery Plan (Sec- tion 31.0) from Security Policy Manual, replaced by Kaseware Contingency Planning Policy.
3.1	3/12/2022	Scott Schons	Annual Review/Update 7.2.1.7
3.2	8/23/2022	Scott Schons	7.2.1.7 Customer Notification

Table of Contents

1 PURPOSE	1
2 SCOPE	1
3 ROLES AND RESPONSIBILITIES	1
4 MANAGEMENT COMMITMENT	2
5 COORDINATION.....	2
6 COMPLIANCE.....	2
7 CONTINGENCY PLANNING POLICY (CP).....	2
8 RELATED POLICIES AND PROCEDURES	6
9 EXCEPTIONS.....	6
10 POLICY APPROVAL	6

1 Purpose

Contingency Planning is required within an organization to provide a process to ensure a calm and complete recovery of the information in the event of a loss of use of that information system. This information is used by government clients to help meet their requirements for Federal Information Security Management Act (FISMA).

All members of Kaseware, Inc. are required to protect applications, information assets, IT Resources and infrastructure against improper or unauthorized access which could result in compromise of confidentiality, integrity and availability of data and IT Resources.

2 Scope

This policy applies to all members of Kaseware, Inc. and all users of any Kaseware applications.

3 Roles and Responsibilities

It is the responsibility of managers to have the appropriate combination of controls (administrative, technical, physical) in effect that provide reasonable assurance that security objectives are addressed.

While a manager may delegate this responsibility, the manager remains accountable.

- Executive Director of Finance and Security
 - a. Ensure that Contingency Plan is conducted for each required client
 - b. Provide needed tools to be used for the Configuration Management
- Director of Technical Operations
 - a. Provide network diagrams
 - b. Provide procedures for networking equipment
- Executive Director of Finance and Security
 - a. Ensure policy is enforced
 - b. Track changes made to this policy
 - c. Ensure compliance of this policy within the environment
 - d. Ensure policy is updated at least annually or when needed
 - e. Ensure the Contingency Plan is tested for each required client
 - f. Manage the Contingency Plan process
 - g. Ensure that the policy is adhered to by system all users Intervene in activities that appear

- to be or are known to be in conflict with this policy
- h. Assist with the management of the Contingency Plan process

4 Management Commitment

This policy is to be updated on an at least annual basis, or when a significant change has occurred within the environment that would force a change to this policy.

As indicated on the signature page at the end of this document, Kaseware, Inc. management has indicated their commitment to ensure that the policy will be adhered to by all members of the organization that report to them.

5 Coordination

This policy will be implemented in a coordinated manner throughout Kaseware, Inc. or outside organization as needed. This coordination will be conducted by the manager who is assigned the primary responsibility for this policy.

6 Compliance

This policy is required and provided for in accordance with regulatory guidance:

NIST Special Publication 800-53, Revision 4

7 Contingency Planning Policy (CP)

7.1. Kaseware, Inc. (CP-1 – CONTINGENCY PLANNING POLICY AND PROCEDURES):

7.1.1. Develops, documents, and disseminates:

- 7.1.1.1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- 7.1.1.2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

7.1.2. Reviews and updates the current:

- 7.1.2.1. Contingency planning policy; and

- 7.1.2.2. Contingency planning procedures.

7.2. Kaseware, Inc. (CP-2 – CONTINGENCY PLAN):

7.2.1. Develops a contingency plan for the information system that:

7.2.1.1. Identifies essential missions and business functions and associated contingency requirements;

7.2.1.1.1. Defines criticality of services in the following order: 7.2.1.1.1.1. Kaseware Production Servers;

7.2.1.1.1.2. Kaseware Demo Servers;

7.2.1.1.1.3. Kaseware Development

Servers; 7.2.1.1.1.4. Kaseware Email and Google Drive.

7.2.1.2. Provides recovery objectives, restoration priorities, and metrics;

7.2.1.2.1. Recovery point objective of 1 hour;

7.2.1.2.2. Recovery time objective of 4 hours;

7.2.1.2.3. Kaseware Production Servers are highest priority.

7.2.1.3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

7.2.1.3.1. Computer Emergency Response Plan requires notification to the CEO, COO, and Director of Technical Operations within 1 hour of identification of emergency.

7.2.1.3.2. The CEO, COO and Director of Technical Operations are responsible for developing an emergency response plan and remediation plan.

7.2.1.3.3. In an emergency, the CEO and COO are authorized to take any and all reasonable actions to prevent system outages and protect integrity of Kaseware systems.

7.2.1.3.4. The CEO in consultation with Kaseware, Inc. outside legal counsel will handle all media requests.

7.2.1.3.4.1. The CEO and COO should consult each other when possible before performing any action.

7.2.1.4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

7.2.1.5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

7.2.1.6. Is reviewed and approved by Kaseware, Inc. Chief Operating Officer.

7.2.1.7. Notifies customers of events which impact customers within 24 hours of event.

- 7.2.1.7.1. Customers will be notified via email and telephone.
- 7.2.2. Distributes copies of the contingency plan;
- 7.2.3. Coordinates contingency planning activities with incident handling activities;
- 7.2.4. Reviews the contingency plan for the information system;
- 7.2.5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
- 7.2.6. Communicates contingency plan changes to the IT management staff including the Director of Technical Operations, Director of Security and Compliance, and Chief Operating Officer; and
- 7.2.7. Protects the contingency plan from unauthorized disclosure and modification.
- 7.3. Kaseware, Inc. (CP-3 – CONTINGENCY TRAINING) provides contingency training to information system users consistent with assigned roles and responsibilities:
 - 7.3.1. Within 90 days of assuming a contingency role or responsibility;
 - 7.3.2. When required by information system changes; and thereafter.
- 7.4. Kaseware, Inc. (CP-4 – CONTINGENCY PLAN TESTING):
 - 7.4.1. Tests the contingency plan for the information system using checklists and an annual walk-through exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan;
 - 7.4.2. Reviews the contingency plan test results; and
 - 7.4.3. Initiates corrective actions, if needed.
- 7.5. Kaseware, Inc. (CP-6 – ALTERNATE STORAGE SITE):
 - 7.5.1. Kaseware, Inc. Production Server data is stored on Microsoft Azure Cloud which eliminates the need for an alternate storage site; and
 - 7.5.2. Kaseware, Inc. relies on security safeguards implemented by Microsoft for Azure servers.
- 7.6. Kaseware, Inc. (CP-7 – ALTERNATE PROCESSING SITE):
 - 7.6.1. Kaseware, Inc. Production Server data is stored on Microsoft Azure Cloud which eliminates the need for an alternate processing site and permits the resumption of Kaseware operations within 4 hour recovery time objective when the primary processing capabilities are unavailable;
 - 7.6.2. Kaseware, Inc. relies on security safeguards implemented by Microsoft for Azure servers.
- 7.7. Kaseware, Inc. utilizes Google Voice for telecommunication services. (CP-8 – TELECOMMUNICATIONS SERVICES).

7.8. Kaseware, Inc. (CP-9 – INFORMATION SYSTEM BACKUP):

7.8.1. Utilizes Microsoft Azure geo-replicated storage to back up user-level information contained in the information system. Additionally;

7.8.1.1. The Kaseware database is backed up every hour;

7.8.1.2. Kaseware file attachments are backed up daily.

7.8.2. Utilizes Microsoft Azure geo-replicated storage to back up system-level information contained in the information system;

7.8.3. Utilizes Microsoft Azure geo-replicated storage to back up information system documentation including security-related documentation; and

7.8.4. Protects the confidentiality, integrity, and availability of backup information at storage locations:

7.8.4.1. Kaseware database and file attachment back ups are encrypted and stored on a separate server;

7.8.4.2. Each backup file shall be retained for a minimum of 14 days;

7.8.4.3. Kaseware, Inc.'s Gitlab repository has a distributed backup on each Kaseware, Inc.'s Developer's computers.

7.9. Kaseware, Inc. provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure (CP-10 –

INFORMATION SYSTEM RECOVERY AND RECONSTITUTION).

7.10. This policy is not meant to cover all scenarios. Some situations will have to be handled on a case-by-case basis. This policy applies to all members of Kaseware, Inc..

7.11. All Incident Response procedures will take into account Kaseware, Inc. client requirements, such as government compliance requirements.

8 Related Policies and Procedures

There are no related policies as of the publication of this version.

9 Exceptions



One-off exceptions to this policy should be reported to the manager responsible for this policy. They will create and maintain documentation for the purpose and acceptance of the exception.

10 Policy Approval

Policy Name: **Kaseware Contingency**

Planning Policy Policy Number: **6.0.0**

The following individuals have reviewed and accepted this policy:

Position	Printed Name	Signature	Date
Executive Director of Finance and Security	Scott P. Schons		8/23/2022
Chief Operating Officer	Nathan Burrows		8/23/2022

SCHEDULE G – TRANSITION IN AND OUT

Transition In Plan

Step	Objective	Purpose	Owner
Stakeholder Alignment	Identify State project stakeholders and provide a list to Contractor	Ensures all stakeholders are involved in discovery sessions, collaborative team meetings and other crucial events.	State
Sample Data Repository	Collection of sample data related to case management workflow use cases, data migration and integration scope.	Allows for proper testing and efficient training materials to be developed.	State
Business Analysis	Understand all workflows and processes for all solution user groups	To allow for the solutions design and configuration to match the identified requirements.	State and Contractor
Access	Provide access to relevant components and environments for the integration phase, if applicable.	Necessary for the integration phase in order to design, test and implement integrations.	State

Transition Out Plan

Step	Objective	Purpose	Owner
Training	Completed training for all user groups of the solution.	Will allow sensitive information, architecture, and disaster recovery plans to be shared.	State and Contractor
User Acceptance Testing	Testing and Configuration acceptance from the State	Ensures all stakeholders are familiar with the system and the features that are relevant to them. Signaled complete by testing acceptance from the State.	State and Contractor
Go-Live and System Acceptance	Successful go live of the solution.	Collaborative go-live that involves Contractor successful handing off the solution to the State, that leads to System acceptance.	State
Transition Support	Continuous support of the solution included 24/7 as part of the subscription model.	To provide the State with the support needed to ensure the continued success of the project.	Contractor
Access	Provide access to relevant components and environments for the integration phase, if applicable.	Necessary for the integration phase in order to design, test and implement integrations.	State

SCHEDULE H – FEDERAL PROVISIONS ADDENDUM

This addendum applies to purchases that will be paid for in whole or in part with funds obtained from the federal government. The provisions below are required and the language is not negotiable. If any provision below conflicts with the State's terms and conditions, including any attachments, schedules, or exhibits to the State's Contract, the provisions below take priority to the extent a provision is required by federal law; otherwise, the order of precedence set forth in the Contract applies. Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. Equal Employment Opportunity

If this Contract is a **"federally assisted construction contract"** as defined in [41 CFR Part 60-1.3](#), and except as otherwise may be provided under [41 CFR Part 60](#), then during performance of this Contract, the Contractor agrees as follows:

(1) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

(2) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to

instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

(4) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The Contractor will comply with all provisions of [Executive Order 11246](#) of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The Contractor will furnish all information and reports required by [Executive Order 11246](#) of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this Contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in [Executive Order 11246](#) of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in [Executive Order 11246](#) of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of [Executive Order 11246](#) of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such

direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: *Provided*, that if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

2. Davis-Bacon Act (Prevailing Wage)

If this Contract is a **prime construction contracts** in excess of \$2,000, the Contractor (and its Subcontractors) must comply with the Davis-Bacon Act ([40 USC 3141-3148](#)) as supplemented by Department of Labor regulations ([29 CFR Part 5](#), "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"), and during performance of this Contract the Contractor agrees as follows:

- (1) All transactions regarding this contract shall be done in compliance with the Davis-Bacon Act (40 U.S.C. 3141- 3144, and 3146-3148) and the requirements of 29 C.F.R. pt. 5 as may be applicable. The contractor shall comply with 40 U.S.C. 3141-3144, and 3146-3148 and the requirements of 29 C.F.R. pt. 5 as applicable.
- (2) Contractors are required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.
- (3) Additionally, contractors are required to pay wages not less than once a week.

3. Copeland “Anti-Kickback” Act

If this Contract is a contract for construction or repair work in excess of \$2,000 where the Davis-Bacon Act applies, the Contractor must comply with the Copeland “Anti-Kickback” Act ([40 USC 3145](#)), as supplemented by Department of Labor regulations ([29 CFR Part 3](#), “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”), which prohibits the Contractor and subrecipients from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled, and during performance of this Contract the Contractor agrees as follows:

- (1) Contractor. The Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into this contract.
- (2) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clause above and such other clauses as FEMA or the applicable federal awarding agency may by appropriate instructions require, and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses.
- (3) Breach. A breach of the contract clauses above may be grounds for termination of the contract, and for debarment as a Contractor and Subcontractor as provided in 29 C.F.R. § 5.12.

4. Contract Work Hours and Safety Standards Act

If the Contract is **in excess of \$100,000** and **involves the employment of mechanics or laborers**, the Contractor must comply with [40 USC 3702](#) and [3704](#), as supplemented

by Department of Labor regulations ([29 CFR Part 5](#)), as applicable, and during performance of this Contract the Contractor agrees as follows:

- (1) Overtime requirements. No Contractor or Subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.
- (2) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (1) of this section the Contractor and any Subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such Contractor and Subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (1) of this section, in the sum of \$27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (1) of this section.
- (3) Withholding for unpaid wages and liquidated damages. The State shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the Contractor or Subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (2) of this section.
- (4) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clauses set forth in paragraph (1) through (4) of this section and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier

subcontractor with the clauses set forth in paragraphs (1) through (4) of this section.

5. Rights to Inventions Made Under a Contract or Agreement

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

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

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

Clean Air Act

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

Federal Water Pollution Control Act

- (1) The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
- (2) The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn,

report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.

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

7. Debarment and Suspension

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

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

8. Byrd Anti-Lobbying Amendment

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

9. Procurement of Recovered Materials

Under [2 CFR 200.322](#), Contractors must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act.

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

10. Additional FEMA Contract Provisions.

The following provisions apply to purchases that will be paid for in whole or in part with funds obtained from the Federal Emergency Management Agency (FEMA):

- (1) Access to Records. The following access to records requirements apply to this contract:

- a. The Contractor agrees to provide the State, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.
- b. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.
- c. The Contractor agrees to provide the FEMA Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the contract.
- d. In compliance with the Disaster Recovery Act of 2018, the State and the Contractor acknowledge and agree that no language in this contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

(2) Changes.

See the provisions regarding modifications or change notice in the Contract Terms.

(3) DHS Seal, Logo, And Flags.

The Contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.

(4) Compliance with Federal Law, Regulations, and Executive Orders.

This is an acknowledgement that FEMA financial assistance will be used to fund all or a portion of the contract. The Contractor will comply with all applicable Federal law, regulations, executive orders, FEMA policies, procedures, and directives.

(5) No Obligation by Federal Government.

The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the State, Contractor, or any other party pertaining to any matter resulting from the Contract.”

(6) Program Fraud and False or Fraudulent Statements or Related Acts.

The Contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the Contractor’s actions pertaining to this contract.

SCHEDULE I – ATTACHMENT 1- BYRD ANTI LOBBYING CERTIFICATION

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

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

Certification for Contracts, Grants, Loans, and Cooperative Agreements

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

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

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction

imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

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

Signature of Contractor's Authorized Official

Name and Title of Contractor's Authorized Official

Date