STATE OF MICHIGAN PROCUREMENT
Department Technology, Management and Budget

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **250000000170**

between

THE STATE OF MICHIGAN

and

CONTRACTOR	Socure, Inc.
	885 Tahoe Boulevard, Suite 1
	Incline Village Nevada 89451
	Nate Schneemann
	810-523-9013
	Nate.Schneemann@socure.com
	VS0234387

STATE	Program Manager	Nathan Ebig	DTMB
		517-282-1917	
		EbigN@michigan.gov	
	Contract Administrator	Kristine Mills	DTMB
		517-242-6402	
		MillsK11@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Fraud Analytics and ID Proofing			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
12/9/2024	12/8/2027	5 - 1 Year	12/8/2027
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
□ P-card □ Payment Request (PRC)		□ Other	☒ Yes □ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
THIS IS NOT AN ORDER. This Contract Agreement is awarded as a result of the State's inquiry bearing the solicitation number RFP 240000000439. Orders for Delivery will be issued directly by the Departments through the issuance of a Delivery Order.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION		**$4,101,018.00**	

SOFTWARE CONTRACT TERMS AND CONDITIONS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this "Contract") are agreed to between the State of Michigan (the "**State**") and Socure, Inc. ("**Contractor**"), a Delaware Corporation. This Contract is effective on December 9, 2024 ("**Effective Date**"), and unless terminated, will expire on December 8, 2027 (the "**Term**").

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

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

"**Acceptance**" has the meaning set forth in **Section 9**.

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

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

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

"Approved Third Party Components" means all Third Party Components, specifically identified by Contractor in the Contractor's Bid Response and as part of the State's Security Accreditation Process defined in Schedule E – Data Security Requirements or of which the State is informed under Section 6.

"**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 provided that such Persons shall be employed by or engaged by the State to perform the role and functions of the State.

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

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

"Contract Change" has the meaning set forth in Subsection 2.2. "Change Notice" means a writing executed by the parties to the Contract memorializing a change to the Contract.

"Change Proposal" has the meaning set forth in Subsection 2.2. "Change Request" has the meaning set forth in Subsection 2.2.

"Confidential Information" has the meaning set forth in Subsection 22.1.

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

“Content ” means the content and other information generated by the Services in response to the State Data and provided by Contractor to the State through the Hosted Services.

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

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

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

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

“**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 Schedule A or subsequent Change Notices 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 that are explicitly designated as Customizations in the applicable Statement of Work.

“Digital Accessibility Standards” means the State of Michigan’s Digital Accessibility Standards, located at https://www.michigan.gov/standards. In the event of a change to the Digital Accessibility Standards in effect as of the Effective Date (other than changes to align with WCAG 2.1 Level AA, or changes required to comply with federal law, with which Contractor or the State are obligated to comply) the parties shall work in good faith to agree to a timeline for compliance under the Change Control process under Section 2.2 of the State’s Software Terms and Conditions.

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

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

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

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

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

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

“**Fees**” means the fees set forth in the Pricing Schedule attached as **Schedule B**. “**Financial Audit Period**” has the meaning set forth in **Subsection 23.1.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"PAT" means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to the Digital Accessibility Standards.

"**Permitted Subcontractor**" means any third party hired by Contractor to perform Services for the State under this Contract, which third party has access to, or has the ability to control, 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.

"**RFS**" means the State's Request for Solution designed to solicit responses for Services under this Contract.

"**Services**" means any of the services, including but not limited to, provision of the Service Platform, Support Services, or 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.

"**Service Platform**" means the SaaS platform through which Contractor provides the Services to include, without limitation, the Software

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

"**Software**" means Contractor's software provided to the State, including without limitation Contractor's Service Platform (which is composed of without limitation, software and microservices) and SDK provided under this Contract, 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 Contractor 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, if any, for such Software, or in a Statement of Work.

"**State**" means the State of Michigan.

"**State 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 into the Service Platform, by; uploaded to the Service Platform from; or placed into the Service Platform by; or that is collected by the Service Platform from, stored in the Service Platform from, Processed by the Service Platform from, or provided to the Service Platform from, any device or system of the State or any individuals directed to the Service Platform by the State, for the use of the Services. For clarity, the Parties acknowledge and agree that emails related to the provision of Services will not constitute State Data for the purposes of this Contract, but will be subject to Section 22 to the extent they contain Confidential Information.

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

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

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

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

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

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

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

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

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

“Third Party Components” are components of the Software that will be deployed within the environment in which State Data is processed or stored, if such components are provided to Contractor by a third party or are Open Source Components and have the ability to impact State Data.

“**Transition Period**” has the meaning set forth in **Section 16.** “**Transition Responsibilities**” has the meaning set forth in **Section 16.** “**Unauthorized Removal**” has the meaning set forth in **Subsection 2.5.**

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

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

“Work Product” means all State-specific deliverables that are explicitly designated as Work Product in the applicable Statement of Work.

2. Duties of Contractor. Contractor will provide Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all 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; provided, however, that Contractor shall not be responsible for delays the extent caused by parties other than Contractor or its subcontractors.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Contract generally or any Statement of Work, including changes to the Services and Implementation Plan (each, a "**Contract Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this Section**.**

2.2.1 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:

2.2.1.1 a written description of the proposed Changes to any Deliverables;

2.2.1.2 an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;

2.2.1.3 any additional State Resources Contractor deems necessary to carry out such Changes; and

2.2.1.4 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.

2.2.2 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, each parties' Contractor Administrator will sign a Change Notice**.**,

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

2.2.3.1 require Contractor to perform or provide the Deliverables under the existing Statement of Work without the Change;

2.2.3.2 require Contractor to continue to negotiate a Change Notice;

2.2.3.3 initiate a Dispute Resolution Procedure; or

2.2.3.4 notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Subsection 16.1**.

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

2.2.5 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 Nonconformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

2.2.6 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.

2.3.1 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.

2.3.2 Prior to any Contractor Personnel performing any Services, Contractor will:

2.3.2.1 ensure that such Contractor Personnel have the legal right to work in the United States;

2.3.2.2 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

2.3.2.3 upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel that access, view, control, or in any way interact with State Data or have the ability to control access to State Data, prior to their assignment. The scope is as provided in the Statement of Work 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.

2.3.3 Contractor and all Contractor Personnel that access, view, control, or in any way interact with State Data, or State facilities 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.

Notwithstanding the foregoing, compliance with Schedule E hereof by those that access, view, control, or interact with State Data shall be deemed compliance with this Section's data security requirements related to State Data. In the event of a change to rules, regulations, and policies of the State that require a modification to Schedule E, the Parties will work in good faith to amend Schedule E and to agree to a timeline to achieve compliance with such change.

2.3.4 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.

2.4.1 Contractor Project Manager must:

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

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

2.4.1.3 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.

2.4.2 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.

2.4.3 Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:

2.4.3.1 the State requests in writing the removal of Contractor Project Manager;

2.4.3.2 the State consents in writing to any removal requested by Contractor in writing;

2.4.3.3 Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

2.4.4 Upon the occurrence of any event set forth in **Subsections 2.4(c)(i-iii)** above, Contractor will promptly replace its Contractor Project Manager**.** Such replacement will be subject to the State's prior written approval.

2.5 Contractor’s Key Personnel.

2.5.1 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.

2.5.2 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.

2.5.3 It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to determine and remedy the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 16**, Contractor will issue to the State an amount equal to $25,000 per individual (each, an “**Unauthorized Removal Credit**”).

2.5.4 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 Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) Reserved.

(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:
Kristine Mills 320 S Walnut Street Lansing, MI 48933 millsk11@michigan.gov 517-242-6402	Head of Legal 885 Tahoe Boulevard, Suite 1 Incline Village, NV 89451 legal@socure.com 866-932-9013

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

5 **Software License.**

5.1 **Perpetual License**. Reserved

5.2 **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:

5.2.1 Contractor hereby grants to the State, exercisable by and through its Authorized Users, a nonexclusive, royalty-free, irrevocable (except as may be otherwise expressly provided herein) 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:

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

5.2.1.2 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 (for clarity, Content is not subject to this (ii), it is subject to a separate license as provided below);

5.2.1.3 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

5.2.1.4 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, up to any limits specified in the applicable Statement of Work or Pricing Schedule, be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Subsection 5.2(c)** below.

5.2.1.5 Software Development Kit. In connection with the Services, Contractor may provide State with access to sample code, or software development kits consisting of documentation, redistributable libraries, and upgrades, modified versions, additions, and improvements therefor, if any (collectively, the "SDK") designed to enable software developers to integrate the Services into State's own branded applications and/or website ("Applications"). In addition to the terms and conditions set forth in the Contract, and the applicable documentation, the SDK may only be used internally in connection with modifying State's own branded Applications solely for the purpose of enabling interoperability with the Services.

5.2.2 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. The licenses granted hereunder are subject to the limitations in this Section 5 and Section 56-3.

5.2.3 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. For clarity, the Fees set forth in a Statement of Work or Pricing Schedule will include without limitation all Fees associated with the State's option to allow individual members of the public, who will not be considered Authorized Users for the purposes of this Contract, to upload information to the Software in accordance with the procedures set in this Contract, so that the State may utilize the full scope of the Services. Such Fees will be Contractor's sole and exclusive remedy for use of the Software, including any excess use, in a manner consistent with this Contract.

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

5.4 **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, if any, 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.

5.5 If Contractor has reasonable grounds to believe that the State or any Authorized User is using the Services in violation of any obligation under this Section 5, Contractor may immediately notify State and if State fails to cure or otherwise reasonably resolve the issue(s) to which Contractor provides notice within 15 Business Days, Contractor may suspend the Services until such time as the noticed issue(s) have been reasonably resolved. While the Services may be used to assist the State in its compliance with applicable laws and regulations, the State acknowledges and agrees that it is solely responsible for its own legal and regulatory compliance obligations. The State acknowledges and agrees that it is solely responsible for its own personal information handling practices.

5.6 At Contractor's request, the State must identify the Authorized Users who will be authorized by the State to have access to and use the Services on behalf of State through Contractor's process of registering to use the Services. The State, will take reasonable measures to ensure that only Authorized Users are permitted to access and use the Services on behalf of the State. The State will appoint one Authorized User to be The State's primary agent in authorizing other Authorized User access to the Services. The State may also appoint secondary agents of the State in authorizing other Authorized User access to the Services. Contractor has no obligation to verify the identity of, and the State is solely responsible for the acts of, any person who gains access to the Services by means of the State's authorized access. The State is solely responsible for monitoring Authorized Users' access to and use of the Services, and for any failure by any Authorized User to comply with the Agreement; a failure to comply with the Agreement by an Authorized User is a failure by the State. The State must immediately take all necessary steps, including providing notice to Contractor, to effect the termination of access for any Authorized User (a) if such individual would no longer meet the definition of "Authorized User" hereunder (for example, through separation of employment), (b) if there is any compromise in the security of passwords, or (c) if unauthorized use is suspected or has occurred. A unique API Key shall be required for each unique authorized source of transactions, such as independently operating affiliates, lines of business or third-party referral sources.

6 **Approved Third Party Components**. At least 30 days prior to using new Third Party Components in environments with access to State Data, 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 Approved Third Party Components included in the Software.

7 Intellectual Property Rights

7.1 Ownership Rights in Software

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

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

(i) The State acknowledges that the Services, the Software, the Service Platform, the Documentation, and the Content (“Contractor Property”) are proprietary in nature and owned exclusively by Contractor. This Contract does not confer to the State any right of ownership in the foregoing. The State is welcome to provide suggestions, comments, instructions, ideas and report issues related to the Contractor Property ("Suggestions"), which may influence how Contractor prioritizes its development efforts provided, however, that any and all Suggestions shall be owned exclusively by Contractor. Without limiting the foregoing, Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Contractor Property; and

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

7.1.3 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, including all Intellectual Property Rights arising therefrom or relating thereto, subject to any rights and licenses granted by the State in this Contract.

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:

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

7.2.2 to the extent any Work Product, or Intellectual Property Rights therein, do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

7.2.2.1 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

7.2.2.2 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. If 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.

9.1.1 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. Transactions processed in the production environment for Acceptance Testing will be at no cost to the extent provided in the appliable Statement of Work or Pricing Schedule.

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

9.1.2.1 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

9.1.2.2 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.

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

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

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

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

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

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have 30 Business Days to use the Software in the Operating Environment

(d) and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Nonconformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Nonconformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in Subsection 9.4 and Subsection 9.5; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State Program Managers or their designees.

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

9.4.1 completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

9.4.2 receipt of the State's notice under **Subsection 9. (a)** or **(c)(i)**, identifying any Nonconformities.

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

9.5.1 continue the process set forth in this **Section 9**;

9.5.2 accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably by agreement between the parties to reflect the value of the Software as received relative to the value of the Software had it conformed; or

9.5.3 deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract in accordance with **Section 16**.

9.6 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the Software under **Subsection 9.3(b)**, or **(c)(ii)**. Acceptance of the Software may be conditioned upon System Acceptance, if Contractor is providing Hardware, under the terms of this Contract.

10 Non-Software Acceptance. This Section 10 does not apply to the Content and information provided through the Service Platform.

10.1 **Reserved**.
10.2 **Reserved**.

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

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

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

11 **Assignment.** Except pursuant to a Change of Control under Section 12, Contractor may not assign this Contract or any of its rights or delegate any of its duties or obligations hereunder, voluntarily, or involuntarily, whether by merger (regardless of whether it is the surviving or disappearing entity), conversion, consolidation, dissolution, or operation of law to any other party without the prior written approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other governmental entity if such assignment is made reasonably necessary by operation of controlling law or regulation. If the State determines that a novation of the Contract to a third party is necessary, Contractor will not unreasonably withhold consent 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 control. 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) intentionally omitted;

(d) consummation of a merger or consolidation of Contractor with any other entity

where Contractor is not the surviving 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 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 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 withhold any amounts in dispute provided that the State is then working in good faith to resolve such fee disputes pursuant to the dispute resolution process set forth herein.

13.5 Taxes. State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if the Services purchased under this Agreement are for State's exclusive use. Contractor shall not invoice taxes for which the State has presented a valid exemption certificate and appropriately claimed tax exempt status. State shall provide Contractor with tax exemption certificates for any such exemptions.

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

13.6.1 The Fees will not be increased at any time during the Term 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.

13.6.2 Contractor warrants and agrees that the Fees granted pursuant to this Contract are comparable to, or better than, the equivalent fees (if any on any current non-discounted price list published by Contractor. specifically for SLED (State, Local, Education) customers under published terms similar to those in this Contract (a "SLED Pricelist"). If Contractor publishes a SLED Pricelist with equivalent fees more favorable than those provided to the State hereunder, then this Contract will be deemed amended as of such SLED Pricelist's effective date 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. Terms are "similar" to this Contract if the terms, taken as a whole (i) impose obligations on Contractor no less than those imposed on Contractor under this Contract and (ii) provide benefits to Contractor no greater than those provided to Contractor under this Contract. Fees are "equivalent" if they assume the same volumes, committed payments, durations, products and services, and other financial terms as those provided to the State hereunder. Except to the extent otherwise provided in this Section, and notwithstanding anything to the contrary in the Contract (including Exhibit B - Pricing), prices provided or offered to other customers of Contractor shall have no impact on the Fees hereunder and Contractor is not obligated to inform the State of any such other prices.

14 **Liquidated Damages**.

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

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

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

14.4 Except where a process for crediting or paying a particular liquidated damage may be expressly set forth in this Contract, amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

15. **Stop Work Order**. The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, the State will either:

(a) issue a notice authorizing Contractor to resume work, or

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

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

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

i. The State may terminate this Contract for cause, in whole or in part, if Contractor:

(i) breaches this Contract in a manner that endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel, for clarity, in such circumstances, the State may terminate immediately;

(ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or

(iii) breaches any of its material duties or obligations under this Contract and, except where immediate termination by the State may be expressly set forth in this Contract, fails to cure such breach within thirty days of written notice of such breach from the State. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

ii. If the State terminates this Contract under this **Subsection 16.1**, the State will issue a termination notice specifying whether Contractor must:

1. 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

2. continue to perform for a specified period.

If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Subsection 16.2**.

iii. This Section (c) applies only in the event of termination under Section 16.1(a). The State will only pay for amounts due to Contractor for Services accepted by the State (or in the case of delivery of Content, that is delivered in a manner consistent with this Contract) 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 to the extent otherwise provided herein. 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 will be responsible for damages incurred by the State in properly terminating this Contract for cause under Section 16.1 and for any reasonable attorneys' fees and court costs incurred by the State in enforcing its termination rights hereunder. Such damages may include reasonable administrative costs, reasonable transition costs, and reasonable costs the State incurs to procure the Services from other sources.

16.2 <u>Termination for Convenience</u>. 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 (or in the case of delivery of Content, that is delivered in a manner consistent with this Contract) within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(b) continue to perform in accordance with **Subsection 16.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

16.3 <u>Transition Responsibilities</u>.

(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 services to the State or its designees. Such transition assistance may include but is not limited to:

1. continuing to perform the Services at the established Contract rates;
2. taking all reasonable and necessary measures to transition performance of the work, including provision of services by the State or the State's designee;
3. taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22**, including without limitation, the return or destruction of State Data at the conclusion of the Transition Period; and
4. 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

17 Indemnification

17.1 <u>General Indemnification</u>. 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, or claims, by third parties, and any losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out such actions or claims, to the extent the actions or claims arise out of:

(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 by any Deliverable, or any component thereof, other than State Materials that may be included in any such Deliverable; and

(c) any bodily injury, death, or damage to real or tangible personal property to the extent occurring 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).

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

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding, at its own expense;

(c) employ its own counsel at its own expense; and to

(d) retain control of its own 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 on behalf of the State. Any litigation activity on behalf of the State or any of its subdivisions must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

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

18 **Infringement Remedies**.

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

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

(a) procure for the State the right to continue to use such Deliverable, or component thereof to the full extent contemplated by this Contract; or

(b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Deliverable and all of its components non-infringing while providing fully equivalent features and functionality.

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

(a) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Deliverable provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(b) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to 6 months to allow the State to replace the affected features of the Deliverable without disruption.

18.4 If Contractor directs the State to cease using any Deliverable under **Subsection 18.3,** the State, at its sole discretion, will be entitled to declare such a direction from the Contractor to cease use a material breach of the Contract and may terminate this Contract under **Section 16**. Unless the claim arose against the Deliverable independently of any of the actions specified below, Contractor will have no liability (under Sections 17 or 18) for any claim of infringement arising solely from:

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

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

19 <u>Disclaimer of Damages and Limitation of Liability.</u>

19.1 Disclaimer of Damages. NEITHER PARTY WILL BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

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

19.3 The Contractor's Limitation on Liability. EXCEPT AS EXPRESSLY PROVIDED BELOW IN THIS SECTION 19.3 OR IN SECTION 19.5, IN NO EVENT WILL CONTRACTOR'S AGGREGATE LIABILITY HEREUNDER, 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 OR ANY SERVICES EXCEED THE GREATER OF: (A) TWO TIMES THE AGGREGATE FEES PAID BY THE STATE TO CONTRACTOR UNDER THIS CONTRACT DURING THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE UPON WHICH THE APPLICABLE CAUSE OF ACTION ARISES (THE "ANNUAL CONTRACT VALUE") AND (B) FIVE MILLION DOLLARS ($5,000,000).

NOTWITHSTANDING ANYTHING SET FORTH IN THIS SECTION 19.3 ABOVE, CONTRACTOR'S LIABILITY WITH RESPECT TO "STATE DATA CLAIMS" (DEFINED AS ANY LIABILITIES OR COSTS FOR WHICH CONTRACTOR IS RESPONSIBLE UNDER SECTION 21.5) AND/OR ANY INDEMNIFICATION OBLIGATIONS WILL NOT EXCEED THE GREATER OF: (A) TWENTY-FIVE MILLION DOLLARS ($25,000,000) AND (B) TO THE EXTENT RECOVERABLE UNDER CONTRACTOR'S INSURANCE, TEN TIMES THE ANNUAL CONTRACT VALUE.

NOTWITHSTANDING ANYTHING ELSE SET FORTH IN THIS SECTION 19.3 ABOVE THE LIMITATIONS OF LIABILITY IN THIS SECTION 19.3 SHALL NOT APPLY TO ANY ACTS OF GROSS NEGLIGENCE, AND/OR WILLFUL MISCONDUCT OF CONTRACTOR (TO INCLUDE ANY EMPLOYEE, SUBCONTRACTOR, OR AGENT THEREOF) OR TO ANY LIABILITIES THAT CANNOT BE LIMITED UNDER APPLICABLE LAW.

19.4 CONTRACTOR WILL NOT BE LIABLE FOR ANY, LOSS OR DAMAGE ATTRIBUTABLE TO ANY SERVICE, PRODUCT OR ACTION OF ANY PERSON OTHER THAN CONTRACTOR (TO INCLUDE ANY EMPLOYEE, SUBCONTRACTOR, OR AGENT THEREOF). The parties acknowledge that CONTRACTOR has set its prices and entered into this Contract in reliance upon the limitations of liability and the disclaimers of warranties and damages set forth in this Contract.

The parties acknowledge that the limitation and exclusions of liability and disclaimers specified in this Contract will survive termination of this Agreement.

19.5 THE EXCLUSIONS AND LIMITATIONS ON LIABILITY IN SECTIONS 19.1-19.3 DO NOT LIMIT EITHER PARTY'S LIABILITY FOR ITS USE OF THE INTELLECTUAL PROPERTY OF THE OTHER PARTY IN VIOLATION OF THE EXPRESSED TERMS OF THIS CONTRACT ("MISAPPROPRIATION CLAIMS"). IN NO EVENT WILL EITHER PARTY'S LIABILITY FOR MISAPPROPRIATION CLAIMS EXCEED TWENTY FIVE MILLION DOLLARS ($25,000,000).

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 (that Contractor is or should be aware of), or an officer or director of Contractor or Permitted Subcontractor (that Contractor is or should be aware of), that arises during the term of the Contract that is:

(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. State Data will be treated by Contractor as Confidential Information.

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 or performing the Services, including a license to collect, process, copy, store, transmit, generate, and display State Data only to the extent necessary in the provision or performance 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 or performing 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, mine, distribute, commercially exploit, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. Contractor's misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795. For clarification purposes, use of State Data for the Services will not be considered commercial exploitation.

(e)All data and information derived, or generated by Contractor from processing transactions under this Contract, shall (to the extent it does not contain State Data) be the sole and exclusive property of Contractor and such data and information shall not be considered State Data. However, such data and information, other than Content, shall be subject to the restrictions set forth in this Section 21.3 to the same extent as State Data. Contractor use of Content will be limited, but only to the extent that Contractor will not use Content in any manner that allows (i) it to attribute the Content to, or correlate it with, any specific individual making use of the Services for any purpose other than providing the Services to the State or (ii) any third party to attribute the Content to, or correlate it with, any specific individual making use of the Services provided under this Contract.

This Section 21 survives the termination of this Contract.

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

21.5 Loss or Compromise of Data. In the event Contractor reasonably believes the security, confidentiality, or integrity, 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, have been compromised (an "Incident"), Contractor must, as applicable:

(a) **Notification to State.** In all events, notify the State as soon as practicable, but no later than 24 hours, if Contractor reasonably believes the Incident to have led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, State Data. In such event, Contractor shall investigate the Incident expeditiously and provide the State a summary of its findings.

(b) **Investigation.** In the event Contractor confirms the Incident to have occurred and to have caused the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to State Data (a "Confirmed Incident"), Contractor will (without limiting its obligations under subsection (a)), make its findings available to the State, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise reasonably requested by the State.

(c) **Notice to Individuals.** In the case of a Confirmed Incident involving PII or PHI for which a notice of the Confirmed Incident is required to affected individuals under applicable law, Contractor shall comply with the following:

(i) Contractor shall provide any such notices required of Contractor under applicable law.

(ii) Where such notices are required of the State under applicable law, Contractor shall, if the Confirmed Incident is an At-Fault Confirmed Incident (as defined hereinafter), at the State's election: (1) provide such notices with approval and assistance from the State or (2) reimburse the State for any costs incurred in notifying the affected individuals.

(iii) Notices required hereunder shall be provided in the manner, and on the timelines, required under applicable law. Where a timeline for notices is not specified under applicable law, unless otherwise agreed by the parties, notice shall be provided within 60 days.

(iv) Notification by Contractor 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 any 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, in the event such notice mentions the State, be reviewed and approved by the State in writing prior to its dissemination.

(d) **Additional Requirements for all Incidents.** In the event of any

Incident, Contractor shall perform or take any actions required of Contractor under applicable law as a result of the Incident.

(e) **Additional Requirements for Confirmed Incident.** In the event of a Confirmed Incident where the State Data in question is PII and for which notification is required under Section 21.5(c), Contractor shall:

(i) Use commercially reasonable efforts to recreate lost State Data in the manner and on the schedule set by the State without charge to the State.

(ii) Provide to the State a detailed plan within 10 calendar days of the Incident becoming a Confirmed Incident describing the measures Contractor will undertake to prevent a future occurrence.

(f) **Additional Requirements for At-Fault Confirmed Incident.** An “At-Fault Confirmed Incident” is a Confirmed Incident where the State Data in question is PII, which Confirmed Incident arises from Contractor’s breach of its obligations hereunder. In the event of an At-Fault Confirmed Incident that compromises PII and for which notification is required under Section 21.5(c), Contractor shall:

(i) Provide third-party credit and identity monitoring services to each of the individuals whose PII was compromised for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 12 months following the date of notification to such individuals. For clarification purposes: if credit monitoring for an individual is otherwise being purchased or funded by Contractor for the applicable 12 month period (for example, if the individual’s information was provided to Contractor under another customer’s contract impacted by the Incident and Contractor is providing credit monitoring under that other customer contract), additional credit monitoring for that individual is not required under this Section.

(ii) Pay for any costs incurred by the State as a result of the Incident, including reasonable attorney’s fees; provided that Contractor shall not be responsible for any credit monitoring costs other than the credit monitoring to be purchased by Contractor under Section 21.5(f)(i).

(iii) Without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all third party claims arising from such Incident, 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 such claims.

21.6 The parties agree that any damages arising out of a breach of the terms set forth in this Section 21 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) disclosed in accordance with the Michigan Freedom of Information Act (FOIA;), provided that any such disclosure may be made only in a manner consistent with Section 22.6; (b) already in the possession of the receiving party without an obligation of confidentiality; (b) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (c) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (d) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information of the State. Information that is the property of Contractor hereunder is not Confidential Information of the State.

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

(a) the subcontractor is a Permitted Subcontractor ;

(b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and

(c) Contractor obligates the Permitted Subcontractor a written contract to maintain the State's Confidential Information in confidence.

22.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Section 22. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

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

22.5 Surrender of Confidential Information. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 30 Calendar Days from the date of the disclosing party's written request following such termination or expiration, return to the other party (in the manner provided in the applicable SOW), or destroy any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Upon confirmation from the State of receipt of all data requested hereunder, Contractor must, within 30 days of the State's written request as provided above, 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 necessary, State will inform Contractor and Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within 30 calendar days from the date of request from the State.

22.6 The Contractor acknowledges that this Agreement, as well as any information, deliverables, records, reports, Content provided to the State, and financial records related to this Contract may be public records as defined under Michigan's FOIA, which the State reserves the right to disclose regardless of actual FOIA requests. However, the State will disclose only those public records or portions of public records that are not, in the State's reasonable determination exempt from disclosure under Michigan's FOIA. Nothing set forth herein will, or is intended to, prevent the State from making a disclosure of any information that is necessary to comply with any other applicable law, regulation, or court order, so long as the State provides written notice of the required disclosure promptly upon receipt of any demand for the disclosure, unless such notice is not allowed under the applicable law, regulation, or court order.

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

23.1 Right of Audit. To the extent provided in MCL 18.1470 or otherwise provided in this Contract, 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 to examine, copy, and audit all records related to this Contract that are subject to audit under Section 23.1. 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. All audits will be subject to reasonable security measures of the auditee (which reasonable security measures may include barring auditors from accessing Contractor systems). Nothing set forth herein will, and is not intended to, restrict the legal authority of the Auditor General of the State of Michigan, under the law.

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

(a) Free of charge during the Warranty Period.

(b) Thereafter, for so long as the State elects to receive Support, in consideration of the State's payment of Fees for such services in accordance with the rates set forth in the Pricing Schedule.

25. Data Security Requirements. Throughout the Term and at all times in connection 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 requirements as set forth in **Schedule E** to this Contract.

26. Training. Contractor will provide, at no additional charge, training on the Deliverable provided hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State's request, Contractor will timely provide training for additional Authorized Users or other additional training on the Deliverables 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 where generally provided to Contractor's other customers at no 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 where generally provided to

Contractor's other customers at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions other than those provided free of additional charge. If the State wishes to install any Maintenance Release or New Version for which there will be an additional charge, the State will have the right to have such Maintenance Release or New Version installed, in the State's discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software, other than those provided free of additional charge, will not affect its right to receive Support Services throughout the Term of this Contract.

27.4 Supported Third Party and Open-Source Components. Contractor will utilize only currently supported versions of all Third Party or Open-Source Components.

28. Source Code Escrow. Reserved

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 Request for Solution; 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 contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

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

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

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

(a) Contractor is the legal and beneficial owner or licensee of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

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

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

(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 (other than Contractor’s payment to its licensors, vendors, or subcontractors);

(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, Contractor will comply with Schedule E to test and maintain the Software and Services to protect against:

(i) Harmful Code; or

(ii) Third party or Open-Source Components, other than Approved Third Party Components.

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

(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, as required to conform 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 by Contractor 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 (meaning web sites other than those of Contractor or the State) 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 AND THE SERVICES (INCLUDING THE SERVICE PLATFORM), INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE PARTIES ACKNOWLEDGE THAT THE SERVICES ARE BASED, IN WHOLE OR IN PART, ON THIRD PARTIES' WEBSITES, SERVICES AND ANALYSIS, AND THAT NO WARRANTY MAY BE PROVIDED IN CONNECTION THERETO. FURTHERMORE, EXCEPT AS SET FORTH IN SCHEDULE D (SERVICE LEVEL COMMITMENTS) THE SERVICES (INCLUDING THE SERVICE PLATFORM) ARE PROVIDED TO THE STATE "AS IS", WITH NO WARRANTIES WITH RESPECT TO THE FUNCTIONALITY OF THE SERVICE PLATFORM, ITS OPERABILITY, USE OR ABILITY TO ACTUALLY DETECT IDENTITY THEFT OR FRAUD, AND CONTRACTOR DOES NOT WARRANT THAT THE SERVICES (INCLUDING THE SERVICE PLATFORM) WILL MEET THE STATE'S REQUIREMENTS, THAT THE OPERATION OF THE SERVICE PLATFORM WILL BE UNINTERRUPTED OR THAT THE SERVICE PLATFORM IS ERROR-FREE. THE ENTIRE RISK REGARDING THE QUALITY AND PERFORMANCE OF THE SERVICES (INCLUDING THE SERVICE PLATFORM) IS WITH THE STATE.

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

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

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

duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

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

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

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

36. **Force Majeure**

36.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, 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 **Section 21** (State Data), **22** (Non-Disclosure of Confidential Information), or **17** (Indemnification) of the Contract, Availability Requirement (if Contractor Hosted) defined in the Service Level Agreement, or any data retention or security requirements under the Contract. A Force Majeure Event impacting Contractor's primary systems will not modify or excuse Contractor's failure to comply with its Disaster Recovery and Backup obligations set forth in the Service Level Agreement. A Force Majeure Event impacting Contractor's disaster recovery or backup systems will modify and excuse Contractor's failure to comply with the foregoing obligations only to the extent such failure is caused by a Force Majeure Event impacting the systems necessary to meet such obligations.

(c) The Parties acknowledge and agree that nothing set forth herein shall excuse Contractor compliance with the Disaster Recovery Plan, as set forth in Schedule F.

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; intellectual property; disclaimers of warranties; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

42. Administrative Fee and Reporting

Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made online by check or credit card at: https://www.thepayplace.com/mi/dtmb/adminfee

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

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

43. Extended Purchasing Program. This contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal.

Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

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

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

45. **HIPAA Compliance**. The State and Contractor must comply with all applicable obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if applicable under HIPAA and reasonably necessary to keep the State and Contractor in compliance with HIPAA.

46. **Accessibility Requirements.** This Section 46 applies only to portions of Software with which the State or the public will interact under the Services.

46.1 All Software provided by Contractor under this Contract, including associated content and documentation, must at all times conform to the Digital Accessibility Standards. Contractor must provide a description of conformance with such specifications by providing a completed PAT for each product provided under the Contract. Throughout the Term of the Contract, Contractor must:

(a) maintain compliance with the Digital Accessibility Standards;

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

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

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

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

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

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 the Digital Accessibility Standards. 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 any non-compliance 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 the 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 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 **Subsection 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 third party claims, including reasonable attorneys' fees, costs, and incidental expenses arising therefrom, 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 Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all

rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

52.1 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.

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
Schedule G	Transition Plan
Schedule H	Data Processing Agreement

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 (c) 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.

56. Product Terms. References in this Section 56 to "Customer" mean the State, to "Socure" mean the Contractor, and to "End Users" mean Authorized Users.

1. **Services.**

1.1 The Services and Fees, Generally. The Pricing Schedule shall specify the relevant solutions to be utilized by Customer, and any other limitations or requirements applicable to Customer's use of the Services. Customer may only utilize the Services with respect to individuals residing in the territories described in the Pricing Schedule (the "Territories") and subject to the terms of this Agreement and the applicable solution-specific or Territory-specific addenda. All fees shall be considered earned upon receipt and nonrefundable, except to the extent otherwise provided herein.

1.2 Performance. Reserved

1.3 Feedback Data. Customer hereby agrees to work in good faith to provide reasonable feedback data, which will be State Data, on the types and outcomes of historic transactions.

1.4 Integration and Updates. The Customer will make reasonable effort to integrate with the latest version of each component of the Services (e.g., Socure's Sigma models, APIs or applicable SDKs) promptly following Socure making them generally available and prior to submitting any transactions in the production environment, in accordance with the applicable documentation and with any implementation certification and approval process made available by Socure. Socure may on reasonable notice to the Customer update, modify and change the Services to comply with any applicable legal and regulatory obligations, to address any reasonably held security concerns, to ensure the provision of the Services keeps pace with its most up to date business practices, and to accord with Socure's rights under the terms on which it receives any relevant data from third parties; provided always that in each case Socure shall act in good faith, including only making such changes where it is reasonable to do so in the circumstances.

2. <u>Socure Content</u>.

2.1 Content License. Contractor grants to the State a nonexclusive, non-transferable, royalty-free, irrevocable (except as otherwise provided herein) right and license to use the Content for any and all of the State's governmental purposes whatsoever except that any such use is subject to the limitations in subsections 3.2, 3.3, 3.6, and 5 of this Section 56 and the following:

(a) the State will not sell or commercially exploit the Content;

(b) the State will not share the Content with any third party except that the State may disclose Content to the extent provided in Section 22.6

The Parties further acknowledge and agree that once Content has been produced or distributed in accordance with this License, the State no longer can control access to, or use of, the produced Content.

This Section shall survive termination or expiration of this Contract.

2.2 Customer may use Socure Marks to refer to Socure and the Services. Customer acknowledges that Socure owns all rights related to or arising from Socure's Marks (as defined below), and agrees that any use of Socure's Marks by Customer (to the extent permitted hereunder) will inure solely to Socure's benefit. Except as otherwise expressly stated in this Agreement, nothing in this Agreement will be construed as conferring any license to Socure's Marks. "Socure's Marks" means and includes all registered or trademarked names, marks, brands, logos, designs, trade dress, slogans and other designations Socure uses in connection with its business, services and products.

2.3 Display of Best Matched Entity. Not applicable

2.4 Software Development Kit. In connection with the Services, Socure will provide Customer with access to sample code, or software development kits consisting of documentation, redistributable libraries, and upgrades, modified versions, additions, and improvements therefor, if any (collectively, the "SDK") designed to enable software developers to integrate the Services into Customer's own branded applications and/or website ("Applications"). In addition to the terms and conditions set forth in the Contract, and the applicable documentation, the SDK may only be used internally in connection with modifying Customer's own branded Applications solely for the purpose of enabling interoperability with the Services.

3. Customer Conduct and Compliance. If Socure has reasonable grounds to believe that Customer or any End User is using the Services in violation of any obligation under this Subsection 3, Socure may immediately notify Customer and if Customer fails to cure or otherwise resolve the grounds of which is has been notified within 30 days, Socure may suspend the Services until such time as Customer has cured or otherwise reasonably resolved the alleged issue. While the Services may be used to assist Customer in its compliance with applicable laws and regulations, Customer acknowledges and agrees that Socure is not responsible for customer's legal and regulatory compliance obligations. Customer acknowledges and agrees that Socure is not responsible for Customer's personal information handling practices.

3.1 Access. Reserved

.

3.2 SDN Compliance. Customer will use the Services pursuant to, and only for the purposes set forth in, this Agreement. Customer will not use, nor will Customer permit any End User to use, the Services for any unlawful purpose or in furtherance of any unlawful purpose, or any purpose that does not comply with Socure's Acceptable Uses, as identified in the Socure Acceptable Use Policy in Section 5 of this Section 56.

3.3 Regulated Industries. Customer will not use the Services or the Content in any way that violates U.S. or Michigan laws, regulation or rule and in a manner inconsistent with Subsection 5 of this Section 56.

3.4 Notices and Consents. Customer shall provide all necessary notices and obtain all necessary consents and approvals required pursuant to applicable laws, including as to (i) the transfer of State Data to Socure and its vendors, (ii) the collection and use of such State Data by Socure and its vendors in accordance with this Contract and (iii) the access by Socure or its vendors to Customer Proprietary Network Information ("CPNI" as such term is defined in the Telecommunications Act). Customer warrants that any consumer information processed by Socure in connection with the Services, including without limitation images, device ID, and device and interaction data, is (i) processed by Socure on the basis of the legitimate interests of Socure and Customer under applicable law; (ii) collected by consumer's devices and transferred directly to Socure and/or its authorized vendors; (iii) processed by Socure and/or its authorized vendors for the purposes and pursuant to Customer's instructions, and otherwise for the purposes, set forth in this Agreement, and (iv) retained by Socure after consumers terminate their accounts with Customer. Customer shall (a) ensure its privacy disclosures, including but not limited to website and mobile app privacy policies, accurately reflect and disclose the collection of personal information, including facial images, biometrics, identity documents, device attributes, behavioral information and other data used for fraud detection via the Services, and Socure's processing of consumer information as set forth herein; (b) shall obtain all consents (including express and/or affirmative consents as appropriate) which are or may be required by applicable laws and shall comply with all requirements of such applicable laws (including any consumer notification requirements) necessary; and (c) fully integrate, as reasonably determined by Socure, with the latest versions of each applicable component in accordance with the applicable documentation to enable Socure's collection of legally required consents. This Section will survive the expiration or earlier termination of this Agreement.

3.5 Unauthorized Code. Customer will implement measures consistent with industry standards to prevent the direct or indirect transmission, by the State or its Authorized Users, of Unauthorized Code to Contractor's servers. "Unauthorized Code" means any virus, software program or segment of code, or other programming design, instruction, or routine that permits unauthorized access to any Socure server, or the Services and is intended to damage, detrimentally interfere with, surreptitiously intercept, or expropriate any of the foregoing or any system, data, or personal information.

3.6 Unauthorized Conduct. Customer will not use nor allow Authorized Users to use the Services or the Content in a way that (a) violates or misappropriates rights to property, intellectual property, privacy, publicity, and treatment of personal information as provided in this Contract; (b) is abusive, or obscene; (c) permits the unauthorized use, disclosure or access of/to the Services or Content, including but not limited to (except as expressly permitted by applicable law or this Contract): selling, sublicensing, reverse engineering, distributing or publishing(except that Content may be made public pursuant to Section 22.6), caching/storing to avoid additional queries , or creating derivative works other than for reporting purposes; (d) violates or circumvents contractual usage or any monitoring, reporting, or authentication mechanisms; (e) or circumvents, breaches, probes or compromises any privacy or security measures, (f) gains unauthorized access to any information, services or systems (such as through phishing, pharming or spoofing), (g) disrupts the integrity, availability or operation of any information, services or systems (e.g. DoS, DDoS), or (h) removes, obscures or circumvents any copyright or other intellectual property notices. This Section shall not make the State responsible for the acts or omissions of a party that utilizes Content in violation of this Section if such party gains access to the Content as a result of such Content being made public pursuant to Section 22.6 (Disclosure pursuant to Michigan's FOIA).

3.7 International Services. The Parties hereto agree to comply with all terms set forth in the Data Processing Agreement, attached hereto as Schedule H.

4. Audit. Socure, upon reasonable advance notice to Customer, at its sole cost and expense, may make a reasonable request for information regarding Customer's compliance with this Agreement, but no more frequently than once during a twelve (12) month period. If any such request for information by Socure results in Socure's belief that Customer is not in compliance with any of Customer's obligations under this Agreement, Socure, will provide notice of any such nonconformance and if such nonconformance has not been cured within 30 days, may suspend Services until such nonconformance is remedied.

5. Acceptable Use Policy. Customer agrees to comply with the following limitations on the use of data provided by the Services: (a) not to use the Services for any "permissible purpose" covered by the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.) ("FCRA") or use any of the information it receives through the Services to take any "adverse action", as that term is defined in the FCRA; (b) not to use the Services in violation of the Driver's Privacy Protection Act (18 U.S.C. Section 2721 et seq.); (c) not to use the Services in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. ("BIPA"), and similar and/or associated laws, whether state, local, foreign, or domestic; (d) not to use the Services other than pursuant to an exception to the privacy provisions of the Gramm-Leach-Bliley Act (15 U.S.C. Sec. 6801 et seq.); and (e) not to use the Services in violation of such other legislation that may be enacted in the future that Socure determines limits the use of the Services by Company. Contractor will not use the information gathered through the Services that include GLBA or DPPA governed data for marketing purposes. Customer shall provide all necessary notices and obtain all necessary consents and approvals required pursuant to applicable laws.

A. GRAMM-LEACH-BLILEY ACT (GLBA) ACCEPTABLE USES

The Contractor’s Services may provide Contractor with access to information that may contain consumer identification information governed by the Gramm-Leach-Bliley Act ("GLBA"). In accordance with the GLBA, Customer certifies that such information will only be used by Customer for the following purposes:

- Fraud detection and prevention purposes including use to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability.
- Completion of a transaction authorized by the consumer including but not limited to the collection of delinquent accounts.
- Application Verification including but not limited to (a) employment application verification (however, such data cannot be used to make an employment decision as outlined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.)), (b) property leasing application information verification (however, such data cannot be used for making a leasing decision as outlined in the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.)), and (c) insurance application information verification (however, such data cannot be used for making a decision to insure an individual or business as outlined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.)). Customer represents and warrants that Socure data will not be used by Customer for purposes governed by the Fair Credit Reporting Act.
- Required institutional risk control programs including complying with federal, state, or local laws, rules, and other applicable legal requirements.
- Dispute resolution for resolving customer disputes or Inquiries.

B. DRIVER’S PRIVACY PROTECTION ACT (DPPA) ACCEPTABLE USES

The information provided to Customer as part of the Services may contain driver's license and motor vehicle registration information subject to the protections of the Driver's Privacy Protection Act (DPPA). In accordance with DPPA, Customer certifies that such information will only be used for the following purposes:

- Use in the normal course of business, to verify the accuracy of personal information submitted by the individual to the business and, if the submitted information is incorrect, to obtain correct information, but only for the purpose of preventing fraud by, or pursuing legal remedies against, or recovering on a debt or security interest against, the individual. 18 U.S.C. § 2721 (b)(3).
- Use by court or other government agency or entity, acting directly on behalf of a government agency. 18 U.S.C. § 2721 (b)(1).

- Use for any matter regarding motor vehicle or driver safety or theft; to inform an owner of a towed or impounded vehicle. 18 U.S.C. § 2721 (b)(2).
- Use in connection with a civil, criminal, administrative, or arbitral proceeding. 18 U.S.C. § 2721 (b)(4).

- Use by an employer or its agents or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under the Commercial Motor Vehicle Safety Act of 1986. 18 U.S.C. § 2721 (b)(9).
- Use by an insurer or insurance support organization, in connection with claims investigation activities, antifraud activities, rating or underwriting. 18 U.S.C. § 2721 (b)(6).
- Use by a licensed private investigative agency, or licensed security service, for a purpose permitted in items 1 through 6 above. 18 U.S.C. § 2721 (b)(8).
- For use in connection with the operation of private toll transportation facilities. 18 U.S.C. § 2721 (b)(10)

Data & Access Security Guidelines

In order to protect sensitive information, it is essential to implement and enforce effective information security processes and programs. The State shall comply with its own security processes and programs, which shall include the following:

- Administrative, physical, and technical safeguards and controls
- Annual security awareness training for all employees
- Strong access controls
- A security incident response plan, along with tools and procedures for monitoring, detecting, investigating, and reporting security-related events
- Anti-virus software with current definitions scanning employee workstations
- Regular reviews of internal controls.

SCHEDULE A – STATEMENT OF WORK

1. DEFINITIONS

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

Term	Definition
Solution	Deliverables (including but not limited to Software, and Documentation) and Services (including but not limited to Hosting Services, Support Services), singularly or in any combination thereof as set forth in a Statement of Work intended to address the State's needs.
SOM	State of Michigan

2. BACKGROUND

The State of Michigan uses Michigan Enterprise Identity and Access Management system branded as "MiLogin" to provide digital identity services to the state's public users, workers and business users, providing access to over 330 government services. Over the past 3 years, the number of public users accessing digital government services has surged across states. The Covid pandemic acted as a catalyst for increased creation of digital government services and their adoption by public users. The increased digitization of government services and rising sophistication of cyber criminals has exposed the government services to increased fraudulent transactions, identity compromise attacks, bot driven traffic, and proliferation of untrusted or fraudulent identities. In order to address these risks, MiLogin will adopt a strategy of using fraud analytics and robust identity verification solutions to detect and reduce fraud attempts. At the same time, these solutions must be inclusive of serving vulnerable populations, allowing them access to digital government services.

3. PURPOSE

Contractor will provide a *Contractor Hosted* Software as a Service compliant with Schedule E of this Contract The Contractor will provide a NIST IAL2 compliant ID proofing solution that uses Government Issued Identification Document (e.g. State Driver's license, State ID card) and person to image verification. The Contractor will also provide a fraud and behavioral analytics solution.

No Customizations or Work Product are being provided under this Statement of Work.

4. IT ENVIRONMENT RESPONSIBILITIES

Included in **SCHEDULE E – Data Security Requirements;** the Contractor will be required to meet all State PSP's, public and non-public applicable to this Contract, only to the extent provided in Schedule E.

Definitions:

Facilities – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.

Infrastructure – Hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.

Platform – Computing server software components including operating system (OS), middleware (e.g., Java runtime, .NET runtime, integration, etc.), database and other services to host applications.

Application – Software programs which provide functionality for end user and Contractor services.

Storage – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations.

Backup – Storage and services that provide online and offline redundant copies of software and data.

Development - Process of creating, testing and maintaining software components.

Component Matrix	Name all contractor(s) and/or subcontractor(s) providing each contract component
Facilities	Socure, Inc.
Infrastructure	Socure, Inc.
Platform	Socure, Inc.
Application	Socure, Inc.
Storage	AWS, Snowflake
Backup	AWS, Snowflake
Development	Socure, Inc.

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 the Digital Accessibility Standards only to the extent provided in the Software Contract Terms and Conditions.

6. USER TYPE AND CAPACITY

Contractor will work with State staff to scale the solution up or down based on the system needs and current usage. Contractor's Solution will at least meet the expected number of transaction volume of users below:

Fraud Analytics:

MILogin Monthly Assessments Data (Average)

Logins	**Registrations**	**Account Self Reactivation**	**Password Self Resets**
4 Million	100,000	52,000	370,000

MiLogin ID proofing Document Verification:

MILogin Monthly Assessments Data (Average)

Number of ID Proofing Transactions per month
130,000

7. ACCESS CONTROL AND AUTHENTICATION

The Contractor's solution must integrate with the State's MiLogin IT Identity and Access Management (IAM) environment as described in the State of Michigan Administrative Guide (1340.00.020.08 Enterprise Identity and Access Management Services Standard (michigan.gov)
.

Administrative access: Administrative Consoles in the Contractor's solution should support, or provide a roadmap for federation with the SOM MILogin solution for access by SOM personnel, and must support SAML, OpenID or OAuth federated identity protocols for Single Sign On.

8. DATA RETENTION AND REMOVAL

The Solution allows the State to retain all data for the entire length of the Contract.

At the request of the State, Contractor will delete State Data, even data that may be stored off-line or in backups.

The State will have access to its data via the Socure Admin Dashboard to the extent provide below and the Socure Admin Dashboard shall provide the capability to audit, report, and visualize prior transactions. Socure responses may be retrieved and downloaded via the the Socure Admin Dashboard in a batch download process. For data deletion in excess of configured requirements, Contractor will delete data pursuant to the written instructions of the State.

The State's process for extracting State Data from the Contractor will be as follows (also provided in Row 4 of the Transition Out Plan attached hereto):

- State will email support@socure.com a data request outlining the date range and attributes that are needed. Client requests are tracked within Contractor's support system.
- Authorized Contractor personnel will create data extract for requested date range and attributes.
- Contractor will transfer through a Secure File Transfer Protocol (SFTP) as defined and agreed to by the parties.

The State may extract State Data from Contractor at any time during the Term.

9. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes currently supported versions of 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 plug-ins 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, which shall be one of the browsers with greater than 2% traffic per above.

This information can be found at https://www.michigan.gov/browserstats. Please use the most recent calendar quarter to determine browser statistics. Support is required for those desktop and mobile & tablet browsers identified as having over 2% of site traffic.

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

Vendor must process and store all State Data in a manner that is logically separated from non-State Data.

Prior to making any significant changes to the architecture, services, or infrastructure , Contractor will notify the State project team. For collaboration on upgrades, maintenance and change control, the State can engage any member of the Contractor's Account Management team or contact support@socure.com 24/7/365. Additionally, Contractor will meet with State on a quarterly basis to review enhancements to solution configurations that can benefit the identity verification and fraud detection performance. Significant changes include, but are not limited to:

- Changes in system architecture, such as hardware, software or firmware.
- Additions/deletions of system interconnections or information sharing.
- Changes in hosting locations or system support.
- Weakness or deficiencies discovered in currently deployed security controls.

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 to the extent provided in the Software Contract Terms and Conditions

Look and Feel Standards

All software items provided by the Contractor with which the public will interact must adhere to the State of Michigan Application/Site standards in effect as of the date hereof which can be found at https://www.michigan.gov/standards.

Mobile Responsiveness

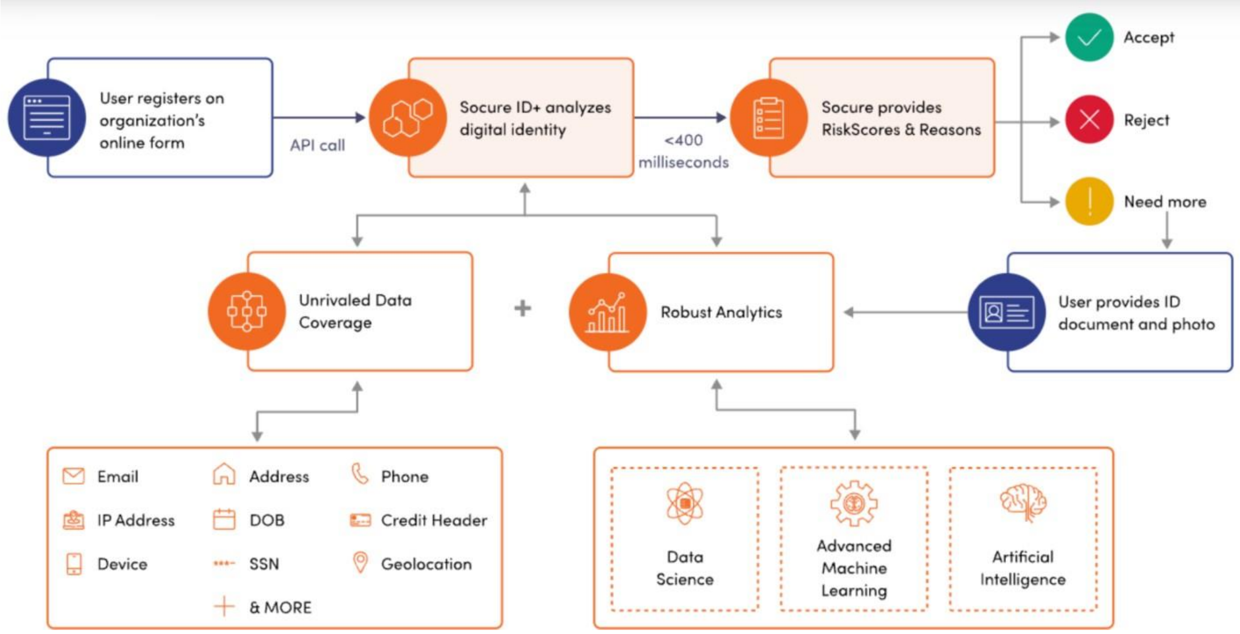
If the software will be used on a mobile device as define in Schedule A – Table 1, Business Specification Worksheet, the Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

SOM IT Environment Access

Contractor will only access State environments from locations within the United States and jurisdictional territories, by using one or more of the following methods:

- Contractor interface with State systems which must be maintained in compliance with State policies and standards as set forth in **Schedule E – Data Security Requirements**.

The diagram below provides a high-level overview of the Socure ID+ solution that Contractor will provide in support of the SOM IT environment and MiLogin.



Contractor will provide development support in the form of both resources and training materials to assist the State in technically integrating the solutions. The Socure Developer's Portal contains all the required training and implementation materials required to support integration activities. Additionally, Technical Account Managers, Developer Support Engineers, Solutions Consultants, and other specialized functions will work with SOM to educate, integrate, and triage SOM technical issues as identified.

Module Overviews

- Socure Verify/Identity Verification – purpose built IDV module that searches and correlates data ingested from sources such as mobile network operators, credit header and credit application data, public records, marketing databases, device information, internet protocol (IP) lists, and telephone port data to return the best- matched identity.
- Sigma Identity Fraud – fraud risk module that employs a ML model trained with 350+ predictors to detect the likelihood of third-party identity fraud. The model analyzes consumer identity dimensions—name, email, phone, address, date of birth, SSN, IP, device, velocity (note that velocity may be unavailable under State terms), network and behavioral intelligence, and more—and then further analyzes how these elements correlate to each other.

- Sigma Synthetic Fraud – utilizes consortium data to tackle fake and randomized synthetic patterns to produce highly accurate, real-time, actionable risk scores, and reason codes, with up to 90% auto-capture in the riskiest 3% of users.
- Email RiskScore – predicts the risk of an email and its correlation to an identity considering hundreds of data elements. Email addresses are correlated with a user's name to establish the prior history and patterns using advanced analytics. Predictive factors include deliverability, legitimacy of host, age of the email, and evaluation as possibly being auto generated by a bot.
- Phone RiskScore – predicts the risk of a phone and its correlation to an identity considering hundreds of data elements. Phones are correlated with a user's name to establish prior history and patterns using advanced analytics. Predictive factors include carrier legitimacy

and velocity (note that velocity may be unavailable under State terms), phone number validity, and length of time a number has been linked to an identity.

- Address RiskScore – predicts the risk of an address and its correlation to an identity considering hundreds of data elements. Addresses are correlated to a user's name to establish residency. Predictive factors include distance from phone area code, distance from IP address, and evaluation of commercial versus residential address.
- Device and Behavioral Risk – predicts risk associated with a device using data attributes such as IP, geolocation, device type, and device software. Device Risk is the first application fraud solution that "binds" a device to the individual using the device to counter application fraud and validate customer logins.
- Socure's Predictive Document Verification (DocV) – digitally verifies the authenticity of thousands of global identity document types from over 190 countries. When combined with a self portrait, DocV can also verify that the biometric and identification card photos match.
- Decision Module – provides a seamless way to orchestrate the breadth of Socure risk scores and reason codes to a client following an identity verification transaction. Socure hosts the decision module and utilizes a client's set risk threshold to help automate decisions to accept, reject, review, resubmit, or refer individuals in an identity verification flow.

Once the ID+ platform cloud services are technically integrated, Contractor and the SOM will assess organizational risk tolerances and determine accept, reject, resubmit and refer to document verification criteria based on Socure's industry best practices and the state's risk posture. These calibrations will be loaded into the Decision Module prior to the go-live date set by the state.

At login, registration, account self reactivation, password resets and other customer identity events the state designed interface will capture and transfer the PII collected via the API to the Socure ID+ module. The module will ingest the PII, conduct applicant analysis, and interpret identity signals via the Decision Module to provide an accept, reject, resubmit and refer attribute that can be returned with the complete risk analysis via the JSON payload. The state will then be able to process the constituent application and flow them through the appropriate user journey.

Contractor will provide, the Socure Admin Dashboard, a portal for the SOM to understand performance and outcomes both at the system and user level. The permission, web-based dashboard is a graphic interface that allows clients to:

- Query the API and view the results;
- Read reports of overall account activity and details of specific transactions;
- Manage users and set up sub-accounts;
- Configure features of certain modules; and
- Assess trends in fraud across populations to make adjustments based on changes to evolving needs and fraud trends.

11. INTEGRATION

Contractor's solution must be capable of integrating with the following:

MiLogin: MiLogin is the Michigan Enterprise Identity and Access Management system. It provides new user registration, authentication and single sign on to agency services and applications, Multi Factor Authentication (MFA), identity verification, and password and account recovery services. Users interact with MiLogin digital identity services via user portals for public users and business users which are currently hosted in the State's private cloud Virtual Data Center and will shortly be migrated to public cloud infrastructure. Additional details on user portals are provided in the table below.

Current Technology	MiLogin's user portals for public users and business users are web applications built on Java, Spring framework, and Angular components.
Volume of Data	The data volumes are described in Section 6.
Format of the input & output interfaces	The MiLogin solution expects to use REST APIs to interact with Fraud Analytics, and Identity Proofing services, and will provide input parameters as part of the API calls and expect the REST APIs to return parameters on results or status. It can also incorporate script snippets in the web applications provided they conform to the technology described above under "Current Technology"

12. RESERVE / MIGRATION

13. RESERVE / HARDWARE

14. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency.

Contractor's training and technical integration support is included with purchase of the ID+ Platform services. Contractor will not limit class attendance. Additional training sessions may be added at no cost as deemed necessary to support the customers development activities.

When preparing for go-live, Contractor will provide the State with recommendations for, and assist the development of the following:

- Best Practices for Decision Logic
- Feedback Template and Returned Sample
- Implementation Certification Document

15. TRANSITION RESPONSIBILITIES

Contractor will provide hands-on guidance to the State in both transition in & out phases. See Schedule G- Transition In and Out for additional details.

16. DOCUMENTATION

Contractor will have documentation to support Socure ID+ including user manuals, technical manuals, installation, and maintenance manuals available 24/7/365 on Socure's Developer's Portal (DevHub). The portal is a web-accessible location, with user permissions managed by the customer administrator via the Socure Admin Dashboard that provides product overviews, API guides, FAQs, release notes and all other applicable content required to integrate the ID+ platform modules. The Socure Admin Dashboard will serve as the centralized portal to view transactions, outcomes, calibrations, customization, and user provisioning options for the Socure products the State is utilizing.

17. RESERVED / ADDITIONAL PRODUCTS AND SERVICES

18. 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
Johnny Ayers, Founder & CEO **885 Tahoe Boulevard, Suite 1** **Incline Village, NV 89451** **410-271-5624** **johnny@socure.com**

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

Contractor
Matt King 885 Tahoe Boulevard, Suite 1 Incline Village, NV 89451 410-271-5624 matt.king@socure.com

19. 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
Laura McGuinn 885 Tahoe Boulevard, Suite 1 Incline Village, NV 89451 914-343-0836 laura.mcguinn@socure.com

Contractor Solution Consultant. Contractor resource who is responsible for overall project implementation. This person will work with the State to define pre-go-live calibrations, coordinate the kickoff meetings, schedule recurring status meetings and will engage additional resources (Development Support Engineers, Data Scientists, etc.) as necessary to solve client related issues.

Contractor
Neal Gallucci 885 Tahoe Boulevard, Suite 1 Incline Village, NV 89451 614-439-0947 neal.gallucci@socure.com

20. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks.

Contractor will have a background check performed on prospective employees. The background investigation will include the following screening criteria:

- Employment history verification
- Criminal background check

- Residency history verification
- Social security number trace
- Sex offender registry check

Contractor will pay for all costs associated with ensuring its staff meet all requirements.

Contractor must notify the State Program Manager(s) prior to removing or replacing any Contractor Personnel with access to State Data under this Contract. Contractor must also provide written certification to the State Program Manager(s) that Contractor Personnel's access to State Data has been terminated.

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

Disclosure of Permitted Subcontractors. If the Contractor intends to utilize subcontractors that are required to be Permitted Subcontractors (as defined in the Contract), the Contractor must disclose the following:

- The legal business name; address; telephone number; a description of subcontractor's organization and the services it will provide; and information concerning subcontractor's ability to provide the Contract Activities.
- The relationship of the subcontractor to the Contractor.
- Whether the Contractor has a previous working experience with the subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Contract Activities that will be performed or provided by the subcontractor.

Bidder must provide detailed information as requested in the above requirement(s).	
The legal business name, address, telephone number of the subcontractor(s).	Amazon Web Services 410 Terry Avenue North Seattle, WA 98109-5210 Snowflake Inc. Suite 3A 106 East Babcock Street Bozeman, MT 59715
A description of subcontractor's organization and the services it will provide and information concerning subcontractor's ability to provide the Contract Activities.	Subcontractors will provide hosting services to Contractor in their FedRAMP Moderate environments.
The relationship of the subcontractor to the Bidder.	**Subcontractors**

Is the subcontractor a GDBE?	**No**
Whether the Bidder has a previous working experience with the subcontractor. **If yes, provide the details of that previous relationship.**	**The listed subcontractors are part of Contractor's standard commercial solution provided to thousands of customers.**
A complete description of the Contract Activities that will be performed or provided by the subcontractor.	Subcontractors will provide hosting services to Contractor in their FedRAMP Moderate environments.

21. 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
Kristine Mills **517-242-6402** **millsk11@michigan.gov**

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

DTMB Program Manager
Amy Cashen **517-855-1066** **cashena@michigan.gov**

22. 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 regular meetings to ensure ongoing support success.

Contractor will provide an Account Management Team, who will be considered Contractor Personnel, to guide product implementation and post-production release account management. The Technical Account Manager acts as the implementation project manager. Additional Account Team member functions are outlined below:

- Account Executive - manages client relationships, helps communicate priorities and timelines to fellow team members to ensure smooth transition of customer objectives.
- Solutions Consultant - accountable for overall project implementation. Works with Technical Account Manager and Strategic Account Manager to define pre-go-live calibrations. Coordinates preliminary kickoff meetings and will work with Technical Account Manager to schedule recurring status meetings. Engages additional resources (Development Support Engineers, Data Scientists, etc.) as necessary to solve client related issues.
- Technical Account Manager - Socure solutions implementation specialist. Provides training on solutions, guidance on Socure ID+ calibration settings, implements client risk tolerances into Decision Module, provides expertise on technical aspects of integrating into the client environment, explains solution module request/response parameters, and helps troubleshoot client implementation issues as they arise. Responsible for customers Implementation Certification process that enables clients go-live. Will ingest project timelines and align resources to support customer implementation timeline, including post go-live support.
- Strategic Account Manager - participates in Decision Module calibration settings to understand client risk tolerances. Works with Solutions Consultants to understand client history and objectives. Works with customers to understand problem areas, leverages daily client performance reports to measure and monitor performance post go-live.

The Contractor’s Account team will meet regularly with the State before go-live to provide hands-on training and guidance during product implementation. This includes a two-hour hands-on training (in-person or web based) preceding API implementation covering:

- Socure Admin Dashboard Review (Access to Transactions, Reports, User Management)
- DevHub Review (Online User Documentation)

23. PROJECT CONTROL & REPORTS

Once the Project Kick-Off meeting has occurred up until Go-Live, 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
- 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.

24. 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.

Implementation **Documentation**
The Contractor shall provide its standard implementation documentation and shall manage implementation in accordance with such documentation.

Milestones/Deliverables for Implementation
Contractor's implementation and production release account management team support is included in a one-time 'Implementation Fee'. Contractor's Technical Account Manager will work with the State to refine the following customer task timelines in order to support the desired production release goal:

Phase	Key Tasks	Owner	Expected Duration *
Pre-Requisites	Register for Account	Customer	1 Day
	Activate, Provision and Map Models to Account	Socure	
	Access to the Socure Admin Dashboard and DevHub	Customer	
	IPs Safelist (Allowed Domains)	Customer	
Kickoff	Kickoff Meeting, Discussion of Use Cases, Target UAT, Target Live	Customer + Socure	1 Day
Specification	Decision Logic Review and Approval	Customer + Socure	1 Week

	Completing Implementation Certification Document	Customer + Socure	2 Days
Development and Certification	Development and Testing within Sandbox Environment	Customer	1-4 Weeks
	Testing within Certification Environment	Customer	2-5 Days
	Implementation Quality Review and Certification	Customer + Socure	2 Days
Go-Live	Socure Admin Dashboard and DevHub Walkthrough	Customer + Socure	1 Day
	Go-Live in Production	Customer	1 Day
Post Go-Live	Monitor Production Transactions After Go-Live	Socure	4 Weeks
	Automating Good/Fraud performance feedback, setup SFTP	Customer + Socure	1-2 Weeks
	Provide First Feedback File (1 to 6 months after Go- Live)	Customer	2-5 Days
Post Post Production Warranty	Included in the cost of Solution	Socure	Production + 90 calendar days
Production Support Services	Ongoing after Final Acceptance	Socure	Ongoing

*Notwithstanding anything to the contrary in the Contract, time is not of the essence for “Expected Durations”

25. RESERVED / HUMAN CENTERED DESIGN (HCD)

26. 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 – ATTACHMENT 1 – BUSINESS SPECIFICATION WORKSHEET

Contractor must meet all business specifications as set forth in this table.

REQUIRED Column 1	**Column 2**
Fraud Analytics	
1.0	Contractor will process and store all State Data logically separated in a SocureGov Cloud environment.
2.0	Detect bot client traffic using passive risk analysis by assessing bot traffic through velocity, risky browsers, network analytics, and device based risks such as virtual machines. (Note that velocity may be unavailable under State terms)

3.0	**New User Registration Assessment** (aka Account Opening): Generate a risk score for the following conditions using the at leas following risk factors: a. High velocity of access risk, from same client to register multiple new user ids (note that velocity may be unavailable under State terms) b. Synthetic identity risk c. Third party identity masquerade risk d. Client reputation risk based on geo origin, prior history and network knowledgebase e. Email and mobile number reputation, throwaway email address or mobile number, telecom association of person to mobile number f. Client device risk computed through device analytics & identity association g. Usage of proxy servers used to mask geo origin h. User behavioral risk based on anomalous digital interaction, coached and coerced behavior The combination of Socure Verify & Socure Sigma Fraud, & Riskscores conduct real time assessments which evaluate identity, third-party, and synthetic fraud based on the risk signals extracted from PII, device, behavioral, velocity (note that velocity may be unavailable under State terms) & IP location.Solution configuration is performed by Socure & customer representatives. The configuration process entails Socure coding risk & reason code intelligence into the Decision Module ‘accept’, ‘reject’, ‘resubmit’ and ‘refer’ outcomes to identify high risk applications based on policy & historical fraud trends.

4.0	Account Access Assessment: Generate a risk score for existing account access using at least the following risk factors: a. High velocity of access from same client for access attempts with same or different user ids (note that velocity may be unavailable under State terms) b. Impossible time travel during access attempts by same client / user id c. Credential stuffing attempts from a single source or sprayed from multiple sources (for example from a botnet) d. Client reputation risk based on geo origin, prior history and network knowledgebase e. Client device risk computed through device analytics f. Different geo origin from previous Access interactions (break in geo origin pattern) g. Usage of proxy servers to mask geo origin h. User behavioral risk based on anomalous digital interaction, coached and coerced behavior

5.0	The Alert List module will provide a signal mechanism to provide known fraud user id/behavior from the application without configuration or customization.
6.0	Socure’s positive/ negative list will provide the ability for the State to implement IP blocklist, allowlist and geo fencing when generating risk score
7.0	Socure’s ID+ platform JSON responses provide RiskScores and Reason Codes.
8.0	The Socure’s Device Intelligence solution will provide a capability to return back user geo location and device attributes (type, OS). Additional Device information (including operating system, manufacturer, version, etc.) and velocity observances of the device are returned, as well as ingested by the fraud modules to influence the risk score outcome. (Note that velocity may be unavailable under State terms)

9.0	Fraud analytics services will use pre-trained models to detect fraud.
10.0	Provide performance test benchmarks such for example: 99% percentile API call response time for 100,000 assessments per hour and regularly assess performance against those benchmarks.
11.0	SOCURE will supply any code to be inserted on web application pages
12.0	SOCURE will provide a dashboard for fraud analytics showing current and previous analytics including but not limited to risk heat maps, geo location wise scores, and drill down data capability. The Socure Admin Dashboard will be enhanced to provide analytic functionality & insight into the client’s overall performance. Socure will share timelines with the deployment of such functionality. MiLogin to be added to beta testing of new Admin Dashboard analytic functionality and insight into overall performance. Socure provides full customer risk analysis details via the API response for the customer to ingest and add to its current business analytics environment.

13.0	SOCURE will provide an API to retrieve detailed session data and scores to facilitate audit investigations. Detailed transaction reports and reporting of bulk data can be pulled from the Socure Admin Dashboard, ad hoc any time with specific module, scores, reason codes and outcomes.
14.0	Capability for Pre-Production UAT validation of new releases.
MiLogin ID Proofing Document Verification	
15.0	Contractor will process and store all State Data logically separated in a SocureGov Cloud environment.

16.0	Socure’s Predictive Document Verification provides the user a complete government issued ID data capture process that includes computer advanced computer vision to conduct: a. Face and orientation detection b. Real-time guidance, edge detection, and cropping c. Glare, focus, and blur validation d. Accessibility features for visually impaired users and support of WCAG 2.1 AA standard
17.0	Socure Predictive Document Verification module will Verify Authenticity of the Government Issued ID. a. Fake ID detection. b. Image of image detection c. Image alert list for repeat bad actors d. Headshot modification detection. Ensure data matches from both sides of the ID card.

18.0	a. Socure Predictive Document Verification uses Optical Character Recognition & reads the Machine Readable Zone to extract information from the Government issued ID. Optical character recognition b. Barcode and MRZ data extraction c. Machine readable to OCR data Correlation d. Input form data and document data correlation e. Option of Global coverage of ICAO-compliant travel documents and national ID cards f. Natural language processing for real-time adjustments to new formats g. New ID document onboarding <5 days This technology supports all ICAO-compliant travel documents & national ID cards.
19.0	The Solution will pass data captured from Government ID back to MiLogin System through the Predictive Document Verification JSON responses.

20.0	The government ID biometric verification process will perform the following functions: a. Selfie to ID photo match b. Facial liveness detection (NIST PAD L2) c. Reduced bias machine- driven decisioning d. Age discrepancy alert

21.0	SOCURE will provide an API to retrieve detailed session data and scores to facilitate audit investigations. Detailed transaction reports and reporting of bulk data can be pulled from the Socure Admin Dashboard, ad hoc any time with specific module, scores, reason codes and outcomes.
22.0	SOCURE will provide the capability for Pre-Production UAT validation of new releases.
23.0	SOCURE to maintain IAL2 assurance level according to latest NIST standards.

24.0	Vendor will provide a dashboard for fraud analytics showing current and previous analytics including but not limited to risk heat maps, geo location wise scores, and drill down data capability and add MiLogin to **beta testing** of new Admin Dashboard analytic functionality and insight into overall performance.

Transaction Response Times. Response Times shall mean the total time from the time a transaction has been received by Contractor's servers until Contractor's servers provide an HTTP response.

Service	Transaction Response Time for the Purposes of Section 2.4 of Schedule D
The following ID+ Passive PII based Transaction Services: Socure Verify Sigma Identity Fraud Sigma Synthetic Fraud Email RiskScore Phone RiskScore Address RiskScore Alert List	2 seconds
ID+ Active Predictive Document Verification Services	7 seconds

Service	**Information Downloadable from Socure Dashboard**
Socure Verify	PII Attributes Correlation Scores, Risk Scores and Reason codes
Sigma Identity Fraud	Risk Scores and Reason codes
Sigma Synthetic Fraud	Risk Scores and Reason codes
Email RiskScore	Risk Scores, Correlation Scores and Reason codes
Phone RiskScore	Risk Scores, Correlation Scores and Reason codes
Address RiskScore	Risk Scores, Correlation Scores and Reason codes
Alert List	N/A (represented as Reason Codes for Fraud/Identity modules)
ID+ Active Predictive Document Verification Services	Document images, Selfies, Reason codes, OCR Data

SCHEDULE B - PRICING

Price includes all costs for the licensing, support, transactions, implementation, and training for the Solution.

Pricing covers all Base (3) and Option Years (5) of the contract.

The State will be provided with 500 API calls at no cost under Sections 5.2.1.4 and 9.1.1 of the Agreement. No fees due hereunder are considered “prepaid” fees for the purposes of the Agreement.

Fraud Analytics:

MILogin Monthly Assessments Data (Average)

Logins	Registrations	Account Self Reactivation	Password Self Resets
4 Million	100,000	52,000	370,000

MiLogin ID proofing Document Verification:

MILogin Monthly Assessments Data (Average)

Number of ID Proofing Transactions per month
130,000

Potential MiLogin users: 12 million

Revision 6/23/2022

Fraud Analytics		**Base Contract**					
		Year 1		**Year 2**		**Year 3**	
Item	**Annual Quantity**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**
Setup Fee (Invoiced on Contract execution)	1	$ 25,000.00	$ 25,000.00				
Support and Maintenance Fee (Invoiced annually with first invoice on Contract execution)	1	$ 65,000.00	$ 65,000.00	$ 71,500.00	$ 71,500.00	$ 78,650.00	$ 78,650.00
Decision Module Fee (Invoiced annually with first invoice on Contract execution)	1	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00
Bundle 2: Identity Verification + Sigma Identity Fraud + Sigma Synthetic Fraud + Sigma Synthetic Fraud + Address riskScore + Email riskScore + Phone riskScore + Device + AlertList + Reason Codes	1,200,000*	$ 0.3018	$ 362,160.00*	$ 0.3018	$ 362,160.00*	$ 0.3018	$ 362,160.00*
Email riskScore	1,200,000*	$ 0.0380	$ 45,600.00*	$ 0.0380	$ 45,600.00*	$ 0.0380	$ 45,600.00*
Phone riskScore	1,200,000*	$ 0.0380	$ 45,600.00*	$ 0.0380	$ 45,600.00*	$ 0.0380	$ 45,600.00*
Device	48,000,000*	$ 0.0024	$ 115,200*	$ 0.0024	$ 115,200.00*	$ 0.0024	$ 115,200.00*
		$ 668,560.00*		**$ 650,060.00***		**$ 657,210.00***	

MiLogin ID Proofing Document Verification		**Base Contract**					
		Year 1		**Year 2**		**Year 3**	
		Price	**QTY Price**	**Price**	**QTY Price**	**Price**	**QTY Price**
Predictive DocV w/Liveness	1,560,000*	$ 0.4541	$ 708,396.00*	$ 0.4541	$ 708,396.00*	$ 0.4541	$ 708,396.00*
		$ 708,396.00*		**$ 708,396.00***		**$ 708,396.00***	
Total Cost		**$ 1,376,956.00***		**$ 1,358,456.00***		**$ 1,365,606.00***	

*These are projected values only based on estimated quantities. Billed amounts will be based on the transaction amount and actual quantity used.

Fraud Analytics		**Option Years w/ Risk-based Approach**									
		Year 4		**Year 5**		**Year 6**		**Year 7**		**Year 8**	
Item	**Annual Quantity**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**
Setup Fee (Invoiced on Contract execution)	1										
Support and Maintenance Fee (Invoiced annually with first invoice on	1	$81,009.50	$81,009.50	$83,439.79	$83,439.79	$85,942.98	$85,942.98	$88,521.27	$88,521.27	$91,176.91	$91,176.91

Contract execution)											
Decision Module Fee (Invoiced annually with first invoice on Contract execution)	1	$10,300.00	$10,300.00	$10,609.00	$10,609.00	$10,927.27	$10,927.27	$11,255.09	$11,255.09	$11,592.74	$11,592.74
Bundle 2: Identity Verification + Sigma Identity Fraud + Sigma Synthetic Fraud + Sigma Synthetic Fraud + Address riskScore + Email riskScore + Phone riskScore + Device + AlertList + Reason Codes	1,200,000*	$0.3109	$373,080.00*	$0.3202	$384,240.00*	$0.3298	$395,760.00*	$0.3397	$407,640.00*	$0.3499	$419,880.00*
Email riskScore	1,200,000*	$0.0391	$46,920.00*	$0.0403	$48,360.00*	$0.0415	$49,800.00*	$0.0427	$51,240.00*	$0.0440	$52,800.00*
Phone riskScore	1,200,000*	$0.0391	$46,920.00*	$0.0403	$48,360.00*	$0.0415	$49,800.00*	$0.0427	$51,240.00*	$0.0440	$52,800.00*

Device	48,000,000*	$0.0025	$120,000.00*	$0.0026	$124,800.00*	$0.0027	$129,600.00*	$0.0028	$134,400.00*	$0.0029	$139,200.00*
		$678,229.50		$699,808.79		$721,830.25		$744,296.36		$767,449.65	
		Option Years w/ Risk-based Approach									
MiLogin ID Proofing Document Verification		**Year 4**		**Year 5**		**Year 6**		**Year 7**		**Year 8**	
		Unit Price	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**	**Unit Price**	**QTY Price**
Predictive DocV w/Liveness	1,560,000*	$0.4677	$729,612.00*	$0.4817	$751,452.00*	$0.4962	$774,072.00*	$0.5111	$797,316.00*	$0.5264	$821,184.00*
		$729,612.00		$751,452.00		$774,072.00		$797,316.00		$821,184.00	
Total Cost		$1,407,841.50		$1,451,260.79		$1,495,902.25		$1,541,612.36		$1,588,633.65	

*These are projected values only based on estimated quantities. Billed amounts will be based on the transaction amount and actual quantity used.

For illustrative purposes, cost breakdown of MiLogin User Flows

MiLogin User Flow	Socure Module Used	Module Category (based on understanding from Socure T&Cs language)	MiLogin Portals	Pricing (Base Contract)
Create Account/Registration	Device Risk + Email Risk + Phone Risk (when phone is present on user’s profile)	Individual Modules: Device + Email + Phone	Public Portal & Business Portal	0.0024 + 0.0380 + 0.0380
Login	Device Risk	Individual Module: Device		0.0024
Forgot Username	Device Risk	Individual Module: Device		0.0024
Forgot Password	Device Risk	Individual Module: Device		0.0024
Edit Email	Device Risk + Email Risk	Individual Modules: Device + Email		0.0024 + 0.0380
Edit Mobile	Device Risk + Phone Risk	Individual Modules: Device + Phone		0.0024 + 0.0380
Edit SQAs	Device Risk	Individual Module: Device		0.0024
Change Password	Device Risk	Individual Module: Device		0.0024

Enterprise ID Proofing	Device Risk + Email Risk + Phone Risk (when phone is present on user's profile) + KYC + Sigma Synthetic Fraud + Address Risk + Sigma Identity Fraud + DocV	Pre-Packaged Common Module + Individual Module: 'Bundle 2' + DocV		0.3018 + 0.4541

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

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

6. REDERVED

7. RESERVED

8. RESERVED

9. RESERVED

Invoice Requirements
All invoices submitted to the State must include: (a) date; (b) purchase order or delivery order; (c) quantity; (d) description of the Solution; (e) unit price; (f) shipping cost (if any); (g) Contractor-generated invoice number and (h) total price.

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

ADDITIONAL TERMS GOVERNING FEES: The Initial Set-Up Fee shall be invoiced upon the Effective Date. The Annual License Fee(s) shall be invoiced upon the Effective Date and annually thereafter except as otherwise described herein. Transactional Fees are invoiced monthly in arrears, calculated based on usage pursuant to the pricing set forth in the Fee Schedule. All fees are payable on invoice as provided in the Terms and are earned on receipt. Transactional pricing is set forth in the Fee Schedule on a per-call basis either for pre-packaged common use cases of desired module group(s) (e.g. Bundle 2) (described below) or on an individual per module basis (e.g. Email riskScore, Phone riskScore). If a single API call makes calls to multiple modules, Customer will be billed for each module called, except in the case of calls to designated common use cases set forth in the Fee Schedule. If a common use case is not elected prior to making an API call to Socure, pricing will be based on each individual module called. Socure’s ability to provide and support the Services in a timely and automated manner is based on a fully integrated deployment of Socure's Services as described in the Agreement.

Socure, Inc.

SCHEDULE C - INSURANCE REQUIREMENTS

Request for Solution No. 240000000128
MiLogin Fraud Analytics and ID Proofing

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.

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	

Required Limits	Additional Requirements
If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

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

STATE OF MICHIGAN
PROCUREMENT
Michigan.gov/MiProcurement

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 **Subsection 2.1.**

"**Availability Requirement**" has the meaning set forth in **Subsection 2.1.**

"**Available**" has the meaning set forth in **Subsection 2.1.**

"**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 **Subsection 3.9.**

"**Critical Service Error**" has the meaning set forth in **Subsection 3.5, Support Request Table.**

"**Exceptions**" has the meaning set forth in **Subsection 2.2.**

"Hosted Services" means, for the purposes of this Schedule D, the SaaS platform through which Contractor provides the Services.

"High Service Error" has the meaning set forth in **Subsection 3.5, Support Request Table.**

"**Low Service Error**" has the meaning set forth in **Subsection 3.5, Support Request Table.**

"**Medium Service Error**" has the meaning set forth in **Subsection 3.5, Support Request Table.**

"**Resolve**" has the meaning set forth in **Subsection 3.6.**

"**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 **Subsection 2.3.**

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

“**Service Availability Credits**” has the meaning set forth in **Subsection 2.6(a).**

“**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 **Subsection 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 **Subsection 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 24 hours/ 7 days.

“**Support Request**” has the meaning set forth in **Subsection 3.5.**

“**Support Service Level Requirements**” has the meaning set forth in **Subsection 3.4.**

2. Service Availability and Service Availability Credits.

2.1 Availability Requirement. Contractor will make the Hosted Services 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 99.90% 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 are available and operable for access and use by the State and its Authorized Users over the Internet. “**Availability**” has a correlative meaning. “Actual Availability” will be calculated for the Service Period as follows: (Actual Uptime) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) x 100 = Availability.

2.2 Exceptions. No period of Hosted Services non-Availability will be included in calculating Availability to the extent that such non-Availability 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 **Subsection 2.3; or**

(c) failure caused by a Force Majeure Event;

2.3 Scheduled Downtime. Contractor must notify the State at least 30 days in advance of all scheduled outages of the Hosted Services in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than two (2) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time on a Weekend; and (c) occur no more frequently than once per quarter; 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 Hosted Services Response Time. Hosted Services response time, where applicable to a service, shall be specified in the SOW for such service. A failure to meet those response times for 98% of the transactions for the applicable service during any three-hour period shall be a High Service Error.

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 as compared to the Availability Requirement. The report must be in electronic format 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 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 is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will, upon the State's written request to Contractor within 30 days after the end of the month during which such Service Error occurred, which request shall set forth the dates and times of the failure, issue to the State the credits described in the Service Availability Table below. The credit amount will be a percentage based upon the average of the monthly per-transaction fees, which average shall be calculated based on the three months immediately prior to Service Period during which the Service Error occurred("**Service Availability Credits**"). For clarification purposes, credits for lack of Availability will be those specified in the Service Availability Table and no credits shall be due for lack of Availability under the Response and Resolution Time Service Table below. A failure to submit such credit request within such 30 day time period, time being of the essence, will constitute a waiver of such right.

SERVICE AVAILABILITY TABLE

Availability	**Credit of Fees**
≥99.90 %	None
<99.90 % but ≥99.51 %	5 %
<99.51 % but ≥95.00 %	10%
<95.0%	15%

(b) Any Service Availability Credits due under this **Subsection** will be applied on the next applicable invoice, provided, however if there is a credit at the time of termination or expiration of the Contract, Contractor shall pay the credits due to the State hereunder no later than 30 days after such termination or expiration.

(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.

(d) IN NO EVENT WILL THE TOTAL CREDITS DURING ANY CONTRACT QUARTER FOR FAILURE TO ACHIEVE THE SERVICE LEVELS SET FORTH IN THIS SCHEDULE D, INCLUDING SERVICE AVAILABILITY AND SUPPORT REQUESTS, EXCEED A TOTAL OF 25% OF THE TOTAL PER TRANSACTION FEES FOR THE QUARTER DURING WHICH THE FAILURE OCCURED.

3. Support and Maintenance Services. Contractor will provide Hosted Services,Software, and Hardware (if applicable) maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this **Section 3.** 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 email for initial support request and then unlimited telephone support, 24 hours/ 7 days.

(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 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 (which may be done by posting a notice online) that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Subsections 3.5 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 (which may be done by posting a notice online) 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; 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** ("**Support Service Level Requirements**"), and the Contract.

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

SUPPORT REQUEST TABLE

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
Critical Service Error (SEV 1)	(i) A problem has been identified that makes the continued use of one or more systems commercially unreasonable or (ii) A problem may cause loss of data and/or restrict data availability and/or cause significant impact to the State.
High Service Error (SEV 2)	(i) Production system, or environment, or a major portion of the system or environment, is degraded, impeding critical business processing and/or

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
	causing disruption to normal production workflow; (ii) Development is down, disrupting critical development; or (iii) A Severity 3 problem has remained unresolved for 48 hours.
Medium Service Error (SEV 3)	(i) A problem that does not have a major effect on the Services used to support applicable business operations or (ii) A problem for which an acceptable work around exists and is available, and operations can continue in a restricted fashion.
Low Service Error (SEV 4)	(i) General user questions about usage of software or web reporting or (ii) Support issues that don't affect processing

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. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error, as set forth in the Response and Resolution Time Service Table below:

RESPONSE AND RESOLUTION TIME SERVICE TABLE

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	30 minutes	**For Hosted Services and Software** 4 hours	5% of the per transaction Fees for the month in which the initial Service Level Failure begins and 5% of such monthly Fees for each additional hour the corresponding Service Error is not responded to.	5% of the per transaction Fees for the month in which the initial Service Level Failure begins and 5% of such monthly Fees for each additional hour that the corresponding Service Error remains un-Resolved.
High Service Error	2 hours	8 hours	3% of the per transaction Fees for the month in which the initial Service Level Failure begins and 3% of such monthly Fees for each additional hour the corresponding Service Error is not responded to.	3% of the per transaction Fees for the month in which the initial Service Level Failure begins and 3% of such monthly Fees for each additional hour that the corresponding Service Error remains un-Resolved.
Medium Service Error	2 hours if call is received prior to 12:00 p.m.	48 hours	N/A	If Medium Service Error has not been resolved in 10 Business Days, the

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)
	Eastern Time. Otherwise, 3 hours			State may resubmit as a High Service Error.
Low Service Error	1 Business Day	Next scheduled release	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, upon written request of the State no later than 30 days following the Service Period in which such failure occurred, issue to the State the corresponding service credits set forth in **Subsection 3.1** ("**Service Level Credits**") and such credits will be applied against the next applicable invoice, provided, however if there is a credit at the time of termination or expiration of the Contract, Contractor shall pay the credits due to the State hereunder no later than 30 days after such termination or expiration. A failure to submit such credit request within such 30 day time period, time being of the essence, will constitute a waiver of such right.

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. RESERVE

5. Data Storage, Backup, Restoration and Disaster Recovery. Contractor must maintain or cause to be maintained backup redundancy and disaster avoidance and recovery procedures designed to safeguard State Data and the State's other Confidential Information, Contractor's Processing capability and the availability of the Hosted Services, 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.

5.1 Data Storage. Contractor will provide sufficient storage capacity to provide the Hosted Services to the State at no additional cost.

5.2 Data Backup. Subject to any specific requirements set forth in Schedule A, or any subsequent Statement of Work, 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,** or any subsequent Statement of Work. The State shall have access to all State Data held by Contractor and Contractor's responses thereto to the extent provided in Schedule A or any subsequent Statement of Work. Additional data can be viewed in an online dashboard maintained by Contractor that provides a real time snapshot of trends and can be adjusted to the needs of the State.

5.3 Data Restoration. Subject to any specific requirements set forth in Schedule A, or any subsequent Statement of Work, if, due to the actions or inactions of the Contractor or its subcontractors, data restoration that does not impact normal processing of transactions is required , Contractor will promptly notify the State and complete actions required to restore service to full production operation. If requested, Contractor will restore data from a backup upon written notice from the State. Contractor will restore the data within two (2) Business Day of the State's request. Contractor will provide data restorations at its sole cost and expense. Nothing set forth in this Section 5.3 will relieve Contractor of any Service Availability obligations as set forth in this Schedule D.

Nothing in this Section 5 will obligate Contractor to any data storage, retention, or recovery obligations, beyond those set forth in Schedule A, or any subsequent Statement of Work. Notwithstanding the foregoing, data restoration provided under this Section is limited to State Data and Contractor's responses thereto through the Hosted Services.

5.4 Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 4 hours and a Recovery Time Objective (RTO) of 4 hours, provided that the Contractor shall reduce RTO to 2 hours no later than October 2024 (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 written request by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 4;** and provide the State with summaries of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt of written request by the State. 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. Nothing set forth in this Section 5.3 will relieve Contractor of any Service Availability obligations as set forth in this Schedule D.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

Contractor Contact	Position	Telephone Number
Nate Schneemann	Socure - Account Executive Director	810.523.9013
Matt Francis	Socure - Principal Solution Consultant	516.417.9874
Beth Bernardo	Socure - Sr Strategic Account Manager	516.604.6516

STATE OF MICHIGAN
PROCUREMENT
Michigan.gov/MiProcurement

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. For the purposes of this Schedule E, references to Hosted Services or Software refer only to those portions of the Hosted Services or Software (as defined in the Contract), as the case may be, that process, store, control access to or directly impact State Data.

"**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 and has the ability to process, store, control access to or directly impact State Data.

"**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 Personnel comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must, subject to Section 12, at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at https://www.michigan.gov/dtmb/policies/it-policies. In the event of a change to the State PSPs, the State shall so inform Contractor in writing and the parties shall work in good faith as described in Section 12.

This responsibility also extends to all service providers and subcontractors that process, store, control access to, or directly impact State Data, provided that Hosting Providers shall instead be subject to Section 5.1. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

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

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

5.1 If Hosted Services are provided by a Hosting Provider outside the boundary of Contractor's own FedRAMP Moderate compliant solution, ensure such 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 and Contractor does not substitute a FedRAMP Moderate authorized Hosting Provider in its place (subject to the State's right to approve Permitted Subcontractors under the terms of the Contract), the State, at its sole discretion, may either a) request the Contractor to move the Software and State Data to an alternative Hosting Provider approved by the State at

Contractor’s sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause.

5.2 for Hosted Services provided by the Contractor in its environment, maintain either FedRAMP Moderate compliance (as evidenced by an assessment by a FedRAMP-approved third party assessor) or an annual SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs.

5.3 be responsible for the Software and State Data being securely stored, hosted, supported, administered, accessed, developed and backed up in the continental United States, and the data center(s) in which State Data resides is minimally maintained so that each and every capacity component and distribution path in a site can be impacted on a planned basis for maintenance or replacement without impacting operations.

5.4 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, subject to Section 12.1, 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, subject to Section 12.1, in applicable State PSPs;

5.5 Throughout the Term, Contractor must not provide Hardware or Services from the list of excluded parties in the System for Award Management (SAM) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services.

5.6 provide technical and organizational safeguards against accidental, unlawful, forbidden, 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 standards and regulations applicable hereunder or under applicable law;

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 without logical separation (State Data encrypted with an encryption key specific to State Data is considered logically separated) with, or contaminated by, the data of other customers or their users of the Services; and (iii) unauthorized access to any 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), mutual Transport Layer Security (TLS), or comparable State approved mechanisms;

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

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

6. Security Accreditation Process. Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the State's 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, subject to Section 12, 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, as necessary, to create or assist the creation of POAMs, perform related remediation activities subject to Section 12, 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.

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 and any other documentation provided under this Schedule E will be recognized as Contractor's Confidential Information.

8.4 With respect to State Data, Contractor must, subject to Section 12, implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program in compliance with requirements set forth in this Contract.

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, subject to Section 12, analyze, remediate and validate all vulnerabilities identified by the scans as required by the State Web Application Security Standard and other applicable PSPs.

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

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

(a) Contractor must either a) grant the State the right to dynamically scan a deployed version of the Software; or b) in lieu of the State performing the scan, Contractor must dynamically scan a deployed version of the Software using an application scanning tool approved under Contractor’s FedRAMP Moderate authorization, 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 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, subject to Section 12, 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 (subject to Section 12) remediation (for clarification purposes, when software provided by a third party includes open source software or the software of other parties, only the third party will be documented). 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 (subject to Section 12) may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

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

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

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must ensure the infrastructure and applications are scanned using a scanning tool approved under Contractor's FedRAMP Moderate authorization at least monthly and provide the scan's assessments to the State in a format that can be used to track the remediation. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements in Section 12.2.

11. Nonexclusive Remedy for Security Breach.

11.1 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.

12. State Standards.

The parties acknowledge and agree that, as of the Effective Date of this Contract, Contractor has provided, and the parties have agreed that, Contractor's FedRAMP SSP using Moderate Baseline Security and Privacy controls from NIST SP 800-53 & SP 800-53B current revisions (Contractor's FedRAMP SSP) is deemed to meet the controls and control parameter requirements under this Schedule E.

12.1 To the extent this Exhibit requires Contractor to comply with any standard (including, without limitation, PSPs), implement any safeguard, or conduct any remediation that is not required under Contractor's FedRAMP SSP, as may have been modified in a future FedRAMP Authorized SSP : (i) Contractor shall so inform the State; (ii) Contractor and the State shall work in good faith to agree in writing to the extent to which, if any, the standard, safeguard, or remediation shall be accepted, waived or deemed inapplicable; and (iii) in the event the parties cannot so agree:

12.1.1. Contractor will perform under Contractor's FedRAMP SSP, as may have been modified in a future FedRAMP Authorized SSP, or

12.1.2. State may choose to terminate this Contract for convenience under subsection 16.2.

12.2 Where remediation is required hereunder, the timeline for such remediation shall (notwithstanding Section 12.1) be as follows:

- Criticals (CVSS 9-10) within 15 days
- Highs (CVSS 7.0-8.9) within 30 days
- Moderates (CVSS 4.0-6.9) within 60 days
- Lows (CVSS .1-3.9) within 90 days.

SCHEDULE F – DISASTER RECOVERY PLAN

Removed for public copy.

SCHEDULE G – TRANSITION IN AND OUT

The below response provides activities, owners and activities to Transition IN/Transition OUT Socure ID+ platform services. The Socure Account Management Team provides support to State through both phases.

Transition IN Plan		
Step	**Owner**	**Activity Description**
1	**MI DTMB**	**Account Registration:** The MI DTMB Account Owner/Administrator registers for a new account through the Socure Admin Dashboard @ https://dashboard.socure.com. This SOM employee will own the initial account administrator role within the Socure Admin Dashboard. After Socure receives and processes the request (Step 2), Socure will provision the account and notify Michigan when it's ready to be used. At that time, the Michigan Account Owner will set up their additional users within the Socure Admin Dashboard.
2	**Socure**	**Activate, Provision, and Map Models to Account** Socure provisions the account for the corresponding ID+ Platform modules & activates the account for use. Socure notifies the Michigan Account Owner that the account is activated. Activation also provides access to the Developer's Portal resources located at https://developer.socure.com. The Account Owner may set up their additional users within the Socure Admin Dashboard. Socure Solutions Consultants or Technical Account managers provide account access management instructions for the MI DTMB administrator to add additional users via a link to the Developer's Hub.

3	**MI DTMB**	**SOM Administrate Access to Socure Admin Dashboard and DevHub** The Michigan Account Owner will set up their additional users within the Socure Admin Dashboard. Users roles for the following user types have been pre-configured: ● Administrator ● Analyst ● Developer ● Case Analyst ● Case Supervisor The administrator can assign additional user roles with customized rights within the Socure Admin Dashboard to support the integration and post go-live activities.
4	**MI DTMB**	**IPs Safelist (Allowed Domains)** After Users are given permissions within the Socure Admin Dashboard, those with a Developer or Administrator role will need to add IP Addresses of the allowed domains that will be utilized to post to the Socure API Endpoints. Instructions for this activity can be found in the DevHub (Developer Hub Documentation) and links to the instructions will be provided by Socure.
5	**MI DTMB/ Socure**	**Kickoff Meeting, Discussion of Use Cases, Target UAT, Target Live** A 1 hour kickoff meeting is set up between MI DTMB & Socure Account Management Team. The MI DTMB & Socure business & technical stakeholders are introduced, MI DTMB provides timelines and objectives for the identity program, and identifies stakeholders responsible for managing the go-live processes. Socure receives project timelines and associated activities for the API integration and aligns resources to support customer related activities. Socure ID+ Platform Project Planning recurring status meeting cadence and personnel are determined. Socure works with MI DTMB to discuss identity & fraud related concerns, as well as tactical and strategic objectives for the platform.
6	**MI DTMB/ Socure**	**Socure Admin Dashboard and DevHub Walkthrough** Two one-hour sessions are scheduled to walk through the Socure Admin Dashboard and Developer's Portal. We typically recommend this walkthrough and training occur close to when Michigan will "Go Live" with the solution; however, we adapt the

		schedule as appropriate for MI DTMB. This can be conducted concurrently with other activities. As new features or enhancements of features are released we can conduct continuous training for Michigan.
7	**MI DTMB/ Socure**	**Decision Logic Review and Approval** If Socure has performed a Proof of Concept, Data Test or Data Analysis, we evaluate the utility of the Decision Module Logic recommendations as a starting point for go-live configuration. If MI DTMB does not want to use the recommendations, we leverage an industry best practices Decision Module logic as a "starting point" for a Decision Logic discussion and configuration. During the time preceding go-live, Socure will work with MI DTMB to identify a starting logic that matches risk tolerance and the "use case" (account creation, license renewal, etc.) the logic will serve. This is conducted concurrently with other development related activities.
8	**MI DTMB/ Socure**	**Completing the Implementation Certification Document** The certification document is a template we leverage to identify and define activities that support MI DTMB's go-live date. This "living" document is curated together over pre go-live activities and used to ensure appropriate development and testing activities have been conducted to enable a successful production launch. The document is leveraged again pre go-live as a checklist to ensure all parties have completed the required activities to support ID+ Platform integration in a production environment.
9	**MI DTMB**	**Development and Testing within Sandbox Environment** MI DTMB resources will begin API and integration development related activities using the 'Sandbox' environment. API request calls made to the environment using the sandbox API key produce randomized results for our customers to understand and assimilate the JSON data into the SOM technical environment. This activity is typically conducted concurrently with the starting Decision Module Logic definition. Once MI DTMB has reached the end of their API development related activities, the customer will change the API to point to the "Certification" environment.
10	**MI DTMB**	**Testing within Certification Environment**

		The “Certification” environment is a mirror copy of the Socure ID+ Platform production environment where the customer incurs transaction costs. Accessible via a separate API key that is located in the customer’s Socure Admin Dashboard, “Certification” is leveraged for late stage MI DTMB user acceptance testing activities to support production-like results from all ID+ modules. After MI DTMB completes UAT, we agree upon a “Certification” checklist execution date.
11	**MI DTMB/ Socure**	**Quality Review and Certification Process Execution** The Quality Review & Certification process is conducted to ensure that the ID+ platform has been successfully integrated across all of the use cases/web locations the service is utilized. The team reviews: ● Passive ID+ platform module integrations will be reviewed to ensure proper operation ● Device SDK and/or Document Verification SDK integrations - the standard approach is to shadow the Michigan team while they conduct a short demo to show where and how the SDKs have been implemented. ● Decision Module logic is reviewed to ensure MI DTMB configuration understanding and alignment ● Additional deployment related activities may be added based on MI DTMB development & deployment plan. Once complete, Socure will rate limit production environments for MI DTMB production use.
12	**MI DTMB/ Socure**	**Go-Live in Production** As a standard practice, we offer MI DTMB to be live with the team as they deploy the technology changes into their production user experience. Through go-live and until a steady state, business as usual performance is achieved, the Socure Account Management Team works with MI DTMB to support on the basis necessary to support successful launch..

Transition Out Plan

Step	Owner	Activity Description
1	**MI DTMB**	**MI DTMB Provide Notice to Cease Services**

		MI DTMB will notify a member of the Socure Account Management team of the notice to cease services and, to the extent desired by MI, provide a written request for destruction of confidential information. A meeting will be scheduled to consult with MI DTMB on concerns, determine transition plan, stakeholders and dates expected.
2	**Socure**	**Transaction OUT Date Rate Limiting** On the mutually agreed upon date, Socure places rate limits on the Socure ID+ Platform to stop the API from processing transaction requests. The API will no longer provide a response to API request calls which prevents additional/accidental transaction costs.
3	**Socure**	**Socure Admin Dashboard & Developer's Portal Account Restrictions** Socure & MI DTMB will agree on the time and date for Socure to restrict access to our online resources. This action/inaction would be determined by the timeline and needs determined in the transition out activities when we receive the Notice to Stop Services
4	**MI DTMB/ Socure**	**Account Data Export** MI DTMB can export Socure data as provided below. • SOM will email support@socure.com a data request outlining the date range and attributes that are needed. Client requests are tracked within Socure's support system. • Authorized Socure personnel will create data extract for requested date range and attributes. • Socure will transfer through a Secure File Transfer Protocol (SFTP) as defined and agreed to by the parties.
5	**Socure**	**Surrender of Information** **On MI's written request, Socure must** permanently delete all State Data from their systems to the extent provided in the Contract.
6	**MI DTMB/ Socure**	**Last Invoice** Socure provides MI DTMB the final invoice for goods/services. Once MI DTMB settles the FINAL invoice, Transition OUT will be completed.

SCHEDULE H – DATA PROCESSING AGREEMENT (DPA)

References herein to “Customer” mean the State, to “Socure” mean Contractor, and to the “Agreement” mean the Contract to which this DPA is attached and incorporated into as Schedule H.

In the event of any conflict or inconsistency between the provisions of the Agreement and this Schedule with regard to the subject matter of this Schedule, the provisions of this Schedule shall control, provided that nothing in this Schedule DPA limits the responsibilities of the parties otherwise provided under the Agreement.

The terms of this Data Processing Agreement (together with all attachments hereto, the “Schedule” or “DPA”) are incorporated into the Agreement. Except as specifically stated herein, all of the terms, provisions, requirements and specifications contained in the Agreement remain in full force and effect, and the terms of this Schedule are in addition thereto. Capitalized terms used but not herein defined shall have the same meanings as set forth in the Agreement. This Schedule shall survive termination of the Agreement for so long as any Customer Personal Data is retained.

1. **Definitions.** Unless otherwise set out in this DPA, any capitalized terms not defined in this DPA shall have the respective meanings given to them in the Agreement.

   1. “**Customer Personal Data**” means Personal Data contained within Customer Information (defined as State Data in the Agreement).

   2. “**Data Protection Laws**” means all laws relating to the collection, use, retention, disclosure, processing, privacy, and protection of Customer Personal Data that are applicable to Customer, Socure, or the Services (as defined in the Agreement).

   3. “**Data Subject**” means an individual who is the subject of Customer Personal Data (or to whom the Customer Personal Data relates).

   4. “**Data Subject Request**” means a request made by a Data Subject to exercise a right conferred on them in relation to Customer Personal Data by Data Protection Laws.

   5. “**Personal Data**” means any information relating to an identified or identifiable individual. Where the applicable Data Protection Laws provide as such, “Personal Data” may also include any information relating to an identified or identifiable household or device.

   6. “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

   7. “**Sub-processor**” means any sub-contractor engaged by and acting under the instructions of Socure that agrees to receive from and process on behalf of Socure any Customer Personal Data.

2. **Data Processing.**

   a. Socure will only process Customer Personal Data in accordance with: (i) the Agreement, to the extent necessary to provide the Services; and (ii) the Customer’s written instructions contained in the Agreement, unless required by applicable laws.

   b. The Agreement (subject to any changes to the Services agreed in writing between the parties), including this DPA, shall be the Customer’s complete and final instructions to Socure in relation to the processing of Customer Personal Data.

c. Socure shall promptly notify Customer if, in its opinion, an instruction of the Customer infringes Data Protection Laws or if applicable law requires it to process the Customer Personal Data other than in accordance with the Customer's instructions and this DPA.

d. If any modification to this Agreement is required to comply with a material change in Data Protection Law, then either Party may notify the other in writing and propose modifications, and the Parties may renegotiate the terms of this Agreement.

e. Each Party is solely responsible for its own compliance with the Data Protection Laws, including without limitation the lawfulness of any transfer of personal data required to obtain or provide the Services.

f. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired or obtained the Customer Personal Data, including providing any required notices, or obtaining any required consents, to Data Subjects.

3. **The California Consumer Privacy Act.** The parties acknowledge and agree that, where Socure is a service provider for the purposes of the California Consumer Privacy Act of 2018 ("CCPA"): (a) Socure is receiving and utilizing Customer Personal Data for a Business Purpose, as defined in Cal. Civ. Code § 1798.140; (b) Socure shall not "sell" or "share" any Customer Personal Data, as those terms are defined by CCPA; and (c) Socure shall not retain, use, or disclose any Customer Personal Data, except as necessary for the purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or permitted by the CCPA.

4. **Sub-Processors.** Customer agrees that Socure may, to the extent and in the manner provided in the Agreement, engage Sub-processors to process Customer Personal Data in accordance with this DPA in connection with providing the Services.

Data Security. See Agreement

Audits. See Agreement

Requests or Demands from Governmental or Regulatory Bodies. Customer acknowledges that any requests or demands from governmental or regulatory bodies that Socure may receive in connection with its processing of Customer's Personal Data are governed by the Third-Party Requests Section 21.4 of the Agreement.

Data Subject Rights

. Customer shall not forward to Socure any Data Subject Request unless Customer has first verified that the Services were used in connection with the Data Subject. Customer shall notify Socure within 7 days of receipt of any applicable Data Subject Request by emailing the contact specified in Appendix 1 and shall encrypt any Customer Personal Data provided in connection therewith. Socure shall support Customer in responding to applicable Data Subject Requests.

a. Socure shall provide notice to Customer within 7 days of confirming that a Data Subject Request relates to Socure's provision of the Services to Customer. Customer's point of contact for communications related to Data Subject Requests is as specified in Appendix 1. Customer has validated that the contact channel for Data Subject Requests is monitored at all times during regular business hours.

b. Socure shall, except as required (or where prohibited) under applicable law, notify Customer within 7 days if it receives a Data Subject Request and, where possible and applicable, Socure shall provide Customer with commercially reasonable cooperation and assistance as is necessary for Customer to comply with its obligations under the Data Protection Laws in relation to any such Data Subject Request. Customer agrees that Socure's cooperation and assistance obligations may be satisfied by providing Customer with the means to delete, export, or otherwise retrieve Customer Personal Data from Socure systems.

c. Customer shall use its best efforts to respond to and resolve promptly all Data Subject Requests which Socure provides to Customer.

d. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Socure’s provision of assistance under this Section 8.

Data Deletion. Unless otherwise required by applicable laws to which Socure or its Sub-processors are subject, Customer Personal Data will be deleted at the same time and manner in which Customer Information is deleted pursuant to the Agreement.

Cross border transfers.

a. **Global Applicability.** This DPA applies to Socure’s processing of Customer Personal Data for the locations specified in the Order Form(s), regardless of whether the processing involves cross border transfers of such data. The Parties represent that they do not believe the laws and practices in any country to which Customer Personal Data is transferred for purposes of the Agreement will prevent Socure or Customer from fulfilling their obligations under this DPA or applicable Data Protection Laws.

b. **UK, EEA, and Switzerland**. If Socure’s Processing of Personal Data involves the transfer of Personal Data of Customer’s Data Subjects located in the European Economic Area (“EEA”), United Kingdom (“UK”) and/or Switzerland to a country or territory outside of those regions, the Parties acknowledge that Socure is an active participant in the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework. , and hereby incorporate, and agree to comply with, the UK International data transfer addendum to the EU SCCs (the “UK Addendum”) issued by the UK Information Commissioner on February 2, 2022 to the EU SCCs. In such case: (i) Module 1 (Controller to Controller) of the EU SCCs shall apply if Socure is designated as a Controller for a particular processing activity, as set forth in Appendix 1. The Parties further agree that the competent supervisory authority where Module 1 applies is the Irish Data Protection Commission (DPC) for the EEA or the Information Commissioner's Office (ICO) for the UK; (ii) Module 2 (Controller to Processor) of the EU SCCs shall apply if Socure is designated as a Processor for a particular processing activity, as set forth in Appendix 1. The Parties further agree that, with respect to Clause 17, Option 1 is selected, and the governing law shall be the laws of Ireland for the EEA and the laws of England and Wales for the UK; (iii) The Parties agree that Appendix 1 to this DPA provides all relevant information to complete Annexes I & II to the EU SCCs and the Tables in Part 1 of the UK Addendum.

c. **Canada**. If Socure’s Processing of Personal Data involves the transfer of Personal Data of Customer’s Data Subjects located in Canada: (i) Customer acknowledges that it has assessed and found adequate the lawfulness, necessity, and proportionality of the processing of Personal Data in connection with the Services; (ii) Customer acknowledges and agrees that it is fully responsible for providing required notices and obtaining required consents from Data Subjects with regard to the processing of their Personal Data in connection with the Services. Customer will not deploy the Services if it deems any notices of consents provided by Socure to be non-compliant with Canadian Data Protection Laws, unless it has first provided supplemental notices and consents to its customers; (iii) Customer is responsible for conducting all required privacy and data transfer compliance documentation, including Privacy Impact Assessments (PIAs) and Data Transfer Impact Assessments (DTIAs); and (iv) For any Services involving the processing of biometric data, Customer represents and warrants that it has: (a) provided its customers with a non-biometric based alternative means for identification, verification, or fraud prevention; (b) meaningfully informed its customers of the non-biometric alternative means before deploying the Services; and (c) notified any regulators required to receive information relating to its use of a biometric database.

APPENDIX 1 to Schedule DPA

Table 1: Parties

Start date	DPA Effective Date	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)

Parties' details	Full legal name: State of Michigan, Department of Technology Management and Budget, Cybersecurity and Infrastructure Protection division Trading name (if different): Main address (if a company registered address): Michigan State Police Headquarters 7150 Harris Drive | Dimondale, MI 48821 Official registration number (if any) (company number or similar identifier):	Full legal name: Socure Inc. Trading name (if different): N/A Main address (if a company registered address): 885 Tahoe Blvd Suite 1, Incline Village, NV 89451 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Nathan Ebig Job Title: MiLogin Service Manager Contact details including email: ebign@michigan.gov	Full Name: Ambar Chavez Job Title: Global Privacy Lead Contact details including email: privacy@socure.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Yes	No	No	Option 2	14 days	No
2	Yes	No	No	N/A	N/A	Yes
3	No	N/A	N/A	N/A	N/A	N/A
4	No	N/A	N/A	N/A	N/A	N/A

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex I.A: List of Parties:

Importer: Socure

Activities relevant to the data transferred under these Clauses: Providing the Services, as that term is defined in the Agreement.

Role: Processor with respect to the Services, except where Data Protection Law provides that it shall be a Controller with respect to specific processing activities.

Exporter: Customer

Activities relevant to the data transferred under these Clauses: Procuring the Services, as that term is defined in the Agreement.

Role: Controller with respect to individual transactions. No role with respect to Socure machine learning or product development and improvements.

Annex I.B: Description of Transfer:

Categories of data subjects whose personal data is transferred: Data subjects whose personal data is transferred to Socure include Customer's customers and may also, from time to time, include Customer's employees or contractors.

Categories of personal data transferred: Personal data transferred may be any of the data described in the "Collection of Personal Information" section of Socure's Privacy Statement.

Annex I.B: Description of Transfer:

Categories of data subjects whose personal data is transferred: Data subjects whose personal data is transferred to Socure include Customer's customers and may also, from time to time, include Customer's employees or contractors.

Categories of personal data transferred: Personal data transferred may be any of the data described in the "Collection of Personal Information" section of Socure's Privacy Statement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: Sensitive data categories: data revealing racial or ethnic origin, biometric data, and criminal convictions and offenses. Restrictions and safeguards include encryption at rest and in transit, access restrictions, restrictions for onward transfers, and purpose limitation.

Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): The data is transferred on a continuous basis in order for Socure to provide the Services.

Nature of the processing: Processing may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing: The purpose of the data transfer is for Socure to provide the Services set forth in the Agreement. Any further processing is done in accordance with Customer's written instructions, and may include machine learning and product development or improvements.

Period for which the personal data will be retained, or, if not possible, the criteria used to determine that period: The personal data is retained in accordance with the Agreement, but in any event, not longer than 7 years from the date of collection. More information about Socure's data retention practices is available here.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: The nature of the processing is such that the personal data is transferred in order for Socure to perform the Services in accordance with the Agreement. The nature and duration of the processing is set forth in the relevant processor or sub-processor agreements.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: Relevant Certifications include: SOC 2 Type 2, ISO 27001:2013 — for Information Security, ISO 27701:2019 — for Privacy Information Management, ISO 27017:2015 — for Information Security Controls within a Cloud Environment, and ISO 27018:2019 — for Privacy of PII held within a Cloud Environment. Additional Measures are described in [Schedule E to the Agreement.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter: Processors and sub-processors are subject to terms similar to those in this DPA.

Annex III: List of Sub processors (Modules 2 and 3 only):

To be provided upon request.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Importer or Exporter may end this Addendum as set out in Section 19 of UK Addendum.