



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

CONTRACT CHANGE NOTICE

Change Notice Number **1**
 to
 Contract Number **MA24000000587**

CONTRACTOR	KLDiscovery Ontrack LLC d/b/a KLDiscovery
	9023 Columbine Rd
	Eden Prairie MN 55347
	Gideon Kaplan
	9529371107
	Gideon.Kaplan@kldiscovery.com
	VS0010297

STATE	Program Manager	Various	Various
	Contract Administrator	Anna Krupka	DTMB
		(517)855-8801	
		KrupkaA@michigan.gov	

CONTRACT SUMMARY

eDiscovery services for the Department of Attorney General.			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
April 3, 2024	April 19, 2027	5 - 1 Year	April 2, 2027
PAYMENT TERMS		DELIVERY TIMEFRAME	
ALTERNATE PAYMENT OPTIONS		EXTENDED PURCHASING	
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>	0 Years	
CURRENT VALUE		VALUE OF CHANGE NOTICE		ESTIMATED AGGREGATE CONTRACT VALUE
\$3,600,000.00		\$0.00		\$3,600,000.00

DESCRIPTION

Please note the Program Manager or Contract Administrator may have changed, and are reflected on this Change Notice.

Effective 02/01/2026, the contract is amended to incorporate the below updated ADA Compliance Language. This language replaces, in its entirety, the previous WCAG 2.0 Level AA language. No additional funding is required.

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

ADA Compliance Language:

"Accessibility Requirements:

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

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

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

AGENCY	NAME	PHONE	EMAIL
AG	Dustin Senneker	517-335-7573	SennekerD@michigan.gov
DTMB	Michael Weiszbrod		WeiszbrodM@michigan.gov



STATE OF MICHIGAN PROCUREMENT
 Department of Technology, Management, and Budget
 320 South Walnut Street
 PO Box 30026
 Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **24000000587**
 between
 THE STATE OF MICHIGAN
 and

CONTRACTOR	KLDiscovery Ontrack LLC d/b/a KLDiscovery
	9023 Columbine Road
	Eden Prairie, MN 55347
	Gideon Kaplan
	952.937.1107
	Gideon.Kaplan@kldiscovery.com
	VS0010297

STATE	Program Manager	Dustin Senneker	AG
		517-335-7573	
	sennekerd@michigan.gov		
	Contract Administrator	Marisha Curtis	DTMB
517-328-9462			
curtism16@michigan.gov			

CONTRACT SUMMARY			
DESCRIPTION: eDiscovery Document Management			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
4/19/2024	4/19/2027	5, 1-Year	4/19/2027
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45			
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
This Contract Agreement is awarded on the basis of the State's inquiry bearing the solicitation number 220000002763. Orders for Delivery will be issued directly by the Departments through the issuance of a Delivery Order.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			\$3,600,000

Program Managers

for

Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Michael Weiszbrod	517-242-1272	weiszbrodm@michigan.gov
AG	Dustin Senneker	517-335-7573	sennekerd@michigan.gov

CONTRACT NO. 240000000587

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

Agency

Date

SOFTWARE CONTRACT TERMS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this “Contract”) are agreed to between the State of Michigan (the “**State**”) and KLDISCOVERY Ontrack, LLC dba KLDISCOVERY (“**Contractor**”), a Delaware limited liability company. This Contract is effective on April 19th 2024 (“**Effective Date**”), and unless terminated, will expire on April 19th 2027(the “**Term**”).

This Contract may be renewed for up to five (5) 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 Contract Change Notice.]

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

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

“**Acceptance Tests**” means such tests as may be conducted in accordance with **Section 9.1** and a Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

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

“**Allegedly Infringing Materials**” has the meaning set forth in **Section 17.2(b)**.

“**Approved Third Party Components**” means all third party components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Contractor’s Bid Response or as part of the State’s Security Accreditation Process defined in Schedule E – Data Security Schedule.

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

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

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

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

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

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

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

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

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

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

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

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

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

“**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 - Statement of Work to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

“Customization” means State-specific changes to a contracted for and created Software's underlying Source Code or structural data model changes. Customization shall not include any changes, modifications or improvements to existing Software provided under this Contract.

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

“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 Services provided.

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

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

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

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

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

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

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

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

“Integration Testing” has the meaning set forth in **Section 9.2(a)**.

“Intellectual Property Rights” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases as well as Software; (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 if any.

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

“New Version” means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market

generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“Nonconformity” or **“Nonconformities”** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

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

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

“PAT” means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

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

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

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

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

available, or (c) block, erase or destroy. “**Processing**” and “**Processed**” have correlative meanings.

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

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

“**Services**” means any of the services, including but not limited to, provision of Software, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

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

“**Site**” means the physical location designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Software.

“**Software**” means Contractor’s or third party software as set forth in a Statement of Work, and any Maintenance Releases or New Versions provided to the State and any directly contracted and paid for Customizations or Configurations (excluding non-contracted improvements, enhancements or modifications) made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract.

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

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

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

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

“**State Materials**” means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

“Work Product” means everything made or created by Contractor specifically and solely for the State for which is not generally available to Contractor's other customers that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to adaptations of State Data, User Data and any form it may take, contracted for Customizations, application programming interfaces, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

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

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each party's Contract Administrator. The term of each Statement of Work will commence on the parties' full execution of a Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 16**. Contractor acknowledges that time is of

the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required, as set forth in the Contract.

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

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

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

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

- (c) If the parties fail to enter into a Change Notice within 15 Business Days following the State's response to a Change Proposal, the State may, in its discretion:
- (i) require Contractor to perform the Services under a Statement of Work without the Change;
 - (ii) require Contractor to continue to negotiate a Change Notice;
 - (iii) initiate a Dispute Resolution Procedure; or
 - (iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Section 16.1**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

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

2.3 Contractor Personnel.

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

- (b) Prior to any Contractor Personnel performing any Services, Contractor will:
- (i) ensure that such Contractor Personnel have the legal right to work in the United States;

- (ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and
- (iii) upon request, or as otherwise specified in a Statement of Work, Contractor will have performed background checks on all Contractor Personnel prior to their assignment. Any further checks will be agreed upon and the scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel upon agreement with such Personnel. 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 have direct access to any Michigan or Agency onsite database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

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

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

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor

Project Manager, who will be considered Key Personnel of Contractor. Contractor Project Manager will be identified in Schedule A - Statement of Work.

(c) Contractor Project Manager must:

- (i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;
- (ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and
- (iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

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

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

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

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

2.5 Contractor's Key Personnel.

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

event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract to which Contractor will be given the opportunity to cure in 24 to 48 hours, in respect of which the State may elect to terminate this Contract for cause under **Section 16.1**.

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

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection 2.5(c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to provide Services to the State under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

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

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

3. Notices. All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Marisha Curtis 320 S. Walnut St. PO Box 30026 Lansing, MI 48909 curtism16@michigan.gov 517-328-9462	Jay Horowitz 9023 Columbine Road Eden Prairie, MN 55347 +1 917-751-9796 Mobile Jay.Horowitz@KLDDiscovery.com

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

5. Software License.

5.1 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:

(a) Contractor hereby grants to the State, exercisable by and through its Authorized Users, a nonexclusive, royalty-free, irrevocable right and license

during the Term and such additional periods, if any, as Contractor is required to perform Services under this Contract or any Statement of Work, to:

- (i) access and use the Software, including in operation with other software, hardware, systems, networks and services, for the State's business purposes, including for Processing State Data;
- (ii) generate, print, copy, upload, download, store and otherwise Process all GUI, audio, visual, digital and other output, displays and other content as may result from any access to or use of the Software;
- (iii) prepare, reproduce, print, download and use a reasonable number of copies of the Specifications and Documentation for any use of the Software under this Contract for internal use only; and
- (iv) access and use the Software for all such non-production uses and applications as may be necessary or useful for the effective use of the Software hereunder, including for purposes of analysis, initial project development, configuration, integration, testing, training, maintenance, support and repair, which access and use will be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Section 5.2(c)** below.

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

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

5.3 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 5**. Such written certification may occur no more than once in any 24-month period during the Term of

the Contract. The State will respond to any such request within 45 calendar days of receipt. If the State's use is greater than contracted, Contractor may invoice the State for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in **Schedule B**, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

5.4 State License Grant to Contractor. The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work. Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

6. Third Party Components. At least 30 days prior to adding new Third Party Components, Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third Party Components included in the Software.

7. Intellectual Property Rights

7.1 Ownership Rights in Software

- (a) For purposes of this **Section 7** only, the term "Software" does not include Customizations.
- (b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Section 7.1(c)**:
 - (i) Contractor reserves and retains, on behalf the Software owner/publisher, its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software including any modifications or improvements therein, except Work Product; and
 - (ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

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

7.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

- (a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and
- (b) to the extent any Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:
 - (i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and
 - (ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called “moral rights” or rights of *droit moral* with respect to the Work Product. None of these waivers or assignments shall apply to Contractor Software or Intellectual Property.

8. Software Implementation.

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

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver the Software on or prior to the applicable Milestone Date within Contractor's environment. Contractor will provide the State with such notice as is specified in a Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery of the Software. If the State is responsible for Site preparation, which the State shall be for its own environment, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

9. Software Acceptance Testing.

9.1 Acceptance Testing.

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

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

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

9.2 Contractor is solely responsible for all costs and expenses related to Contractor’s performance of, participation in, and observation of Acceptance Testing.

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software (“**Integration Testing**”). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 9.1**, **Section 9.4**, and **Section 9.5**.

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

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

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

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

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

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

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

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Section 9.1(a)** or **Section 9.3(c)(i)**, identifying any Non-Conformities.

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

(a) continue the process set forth in this **Section 9**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract for cause in accordance with **Section 16.1**.

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

10. Non-Software Acceptance.

10.1 All other non-Software Services and Deliverables are subject to inspection and testing by the State within 30 calendar days of the State’s receipt of invoices for them if such inspection and acceptance is noted for a Milestone (“State Review Period”), or unless otherwise provided in the Statement of Work. If the non-Software Services and Deliverables are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the non-Software Services and Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Services and Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the non-Software Services and Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16.1**, Termination for Cause.

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

correct deficiencies in accordance with the time response standards set forth in this Contract.

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

11. Assignment. Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

12. Change of Control. Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

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

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

13. Invoices and Payment.

13.1 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt.

Contractor may only charge for Services and Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Services and Deliverables. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

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

13.4 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

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

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

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

(b) Excluding federal government charges and terms. Contractor warrants and agrees that each of the Fees, economic or product terms or warranties granted pursuant to this Contract are comparable to or better than the equivalent fees, economic or product term or warranty being offered to any government customer (including any public educational institution within the State of Michigan) of Contractor. If Contractor enters into any arrangements with another customer of Contractor to provide the products or services, available under this Contract, under more favorable prices, as the prices may be indicated on Contractor's current U.S. and International price list or

comparable document, then this Contract will be deemed amended as of the date of such other arrangements to incorporate those more favorable prices, and Contractor will immediately notify the State of such Fee and formally memorialize the new pricing in a Change Notice.

14. Liquidated Damages.

14.1 The parties understand and agree that any liquidated damages (which will be solely applicable credits) set forth in this Contract are reasonable estimates of the State's damages in accordance with applicable law.

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

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause under **Section 16.1** and the State will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

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

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

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

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

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

- (a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:
- (i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;
 - (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or
 - (iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.
- (b) If the State terminates this Contract under this **Section 16.1**, the State will issue a termination notice specifying whether Contractor must:
- (i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or
 - (ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 16.2**.
- (c) The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. Further, Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

16.2 Termination for Convenience. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason or no reason, including

but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must:

- (a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or
- (b) continue to perform in accordance with **Section 16.3**. If the State terminates this Contract for convenience, the State will pay all costs for Services performed, as well as all reasonable costs determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

16.3 Transition Responsibilities.

- (a) Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days; the “**Transition Period**”), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to:
 - (i) continuing to perform the Services at the established Contract rates;
 - (ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State’s designee;
 - (iii) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22.5** regarding the return or destruction of State Data at the conclusion of the Transition Period; and
 - (iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the “**Transition Responsibilities**”). The Term of this Contract is automatically extended through the end of the Transition Period.
- (b) Contractor will follow the transition plan attached as **Schedule G** as it pertains to both transition in and transition out activities.

17. Indemnification

17.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification) in accordance with the terms of this Contract, arising out of or relating to:

- (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;
- (b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;
- (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and
- (d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

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

- (a) regular updates on proceeding status;
- (b) participate in the defense of the proceeding;
- (c) employ its own counsel; and to
- (d) retain control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its

subdivisions, under this **Section 17**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

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

18. Infringement Remedies.

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

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

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

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

- (a) refund to the State any pre-paid amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract as of the date of the infringement; 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 3 month to allow the State to replace the affected features of the Software without disruption.

18.4 If Contractor directs the State to cease using any Software under **Section 18.3**, the State may terminate this Contract for cause under **Section 16.1**. Unless the claim arose against the Software independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

- (a) Contractor's compliance with any designs, specifications, or instructions of the State; or
- (b) modification of the Software by the State without the prior knowledge and approval of Contractor.

19. Disclaimer of Damages and Limitation of Liability.

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

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

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

19.4 The Contractor's Limitation of Liability. IN NO EVENT WILL THE CONTRACTOR'S AGGREGATE LIABILITY TO THE STATE 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 \$15,000,000 (FIFTEEN MILLION) PER CLAIM OR SERIES OF RELATED CLAIMS GIVING RISE TO THE DAMAGES.

19.5 Exceptions. Subsections (a) (Disclaimer of Damages) and (b) (Limitation of Liability) above, will not apply to: (i) Contractor's obligation to indemnify under this Contract; (ii) Contractor's obligations under Section 21 of this Contract (Loss or Compromise of State Data); (iii) any loss or claim to the extent the loss or claim is covered by a policy of insurance maintained, or required by this Contract to be maintained, by Contractor to the limits of such coverages; and (iv) damages arising from either party's recklessness, bad faith, or intentional misconduct. As it pertains to sections (i) and (ii) of this part, the total liability of Contractor shall in no event exceed \$25,000,000 (twenty-five million) per claim or series of related claims.

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 which shall affect Contractor's ability to perform under this Contract or that directly impacts the Contractors viability, financial stability or its ability to perform under this Contract (collectively, "**Proceeding**") involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

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

21. State Data.

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

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

- (i) personally identifiable information (“**PII**”) collected, used, Processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual’s social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother’s maiden name, email address, credit card information, or an individual’s name in combination with any other of the elements here listed; and
- (ii) protected health information (“**PHI**”) collected, used, Processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act (“**HIPAA**”) and its related rules and regulations.

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

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

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

21.4 Discovery. Contractor will immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State’s use of the Software and Hosted Services, if applicable. Contractor will notify the State

Program Managers or their designees by the fastest means available and also in writing. In no event will Contractor provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for State review, revision and approval.

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

- (a) notify the State as soon as practicable but no later than 24 hours of becoming aware of such occurrence;
- (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;
- (c) in the case of PII or PHI, at the State's sole election:
 - (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or
 - (ii) reimburse the State for any costs in notifying the affected individuals;
- (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;
- (e) perform or take any other actions required to comply with applicable law as a result of the occurrence;
- (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence;

(h) assist the State as much as possible in recreating lost adaptations of State Data in the manner and on the schedule set by the State without charge to the State; and

(i) provide to the State a detailed plan within 10 calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination.

21.6 The parties agree that any damages relating to a breach of **Section 21.6** are to be considered direct damages and not consequential damages.

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

22.1 Meaning of Confidential Information. For the purposes of this Contract, the term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); the

parties note as it relates to records, which shall be the records and systems as well as information security documentation of Contractor, shall be exempt from disclosure under MCL 15.243(y) when applicable; (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

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

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

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

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

22.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 5 Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State's Confidential Information, including State Data, from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. If the State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within 5 Business Days from the date of confirmation from the State.

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

23.1 Right of Audit. Pursuant to MCL 18.1470, the State or its designee may audit with 10 business days advance written notice subject to confidentiality undertakings being given, Contractor to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

23.2 Right of Inspection. Within 10 business days of providing written notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises while accompanied or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are

revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within 45 calendar days.

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

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

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

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

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

27. Maintenance Releases; New Versions

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

27.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all New Versions, each of

which will constitute Software and be subject to the terms and conditions of this Contract.

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

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

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

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

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

(a) RESERVED

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

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

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

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

(i) conflict with or violate any applicable law;

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

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

(f) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as delivered or installed by Contractor does not or will not:

- (i) infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; or
 - (ii) fail to comply with any applicable law;
- (g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:
- (i) Harmful Code; or
 - (ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.
- (h) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and
- (i) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.
- (j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;
- (k) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever;
- (l) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

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

(n) If Contractor Hosted:

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

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

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

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

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

30. Offers of Employment. During the first 12 months of the Contract, should Contractor hire an employee of the State, without prior written consent of the State, who has substantially worked on any project covered by this Contract. The Contractor will be billed for 50% of the employee's annual salary in effect at the time of separation. This shall not apply if an employee of the state responds to a public solicitation for jobs from Contractor.

31. Conflicts and Ethics. Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract;

(b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any Permitted Subcontractor that provides Services and Deliverables in connection with this Contract.

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

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

34. Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

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

36. 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.

37. Force Majeure

37.1 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.

37.2 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 except for payment of services performed prior to Force Majeure event 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.

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

- (a) in no event will any of the following be considered a Force Majeure Event:
 - (i) shutdowns, disruptions or malfunctions of Hosted Services or any of Contractor’s telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Hosted Services; or

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

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

38. 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.

39. 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.

40. 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.

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

42. Survival. Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this

Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification; disclaimer of damages and limitations of liability; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

43. Reserved

44. Reserved

45. Contract Modification. This Contract may not be amended except by signed agreement between the parties (a “**Contract Change Notice**”). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

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

47. Accessibility Requirements.

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

- (a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;
- (b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;
- (c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor’s Software to WCAG 2.0 Level AA;
- (d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor’s Software;

- (e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and
- (f) participate in the State of Michigan Digital Standards Review described below.

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

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

47.4 Reserved

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

48. 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.

49. 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.

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

51. 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.

52. 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 unless such relief is unfounded.

53. Reserved

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

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

55. 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.

56. 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; (b) second, Schedule E – Data Security Requirements; (c) third, Schedule H – HIPAA Business Associate Agreement; (d) fourth, each Statement of Work; and (e) fifth, the remaining Exhibits and Schedules to this Contract. NO TERMS ON CONTRACTOR’S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO STATE’S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A – STATEMENT OF WORK

1. DEFINITIONS

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

Term	Definition
ADA	Americans with Disabilities Act
AG	Department of Attorney General
CAR	Computer Assisted Review
DTMB	Department of Technology, Management, and Budget
EDRM	Electronic Discovery Reference Model
ESI	Electronically Stored Information
POAM	Plan Of Action and Milestones
PAT	Product Accessibility Template
PSP	Policies, Standards, and Procedures
SFTP	Secure File Transfer Protocol
SOM	State of Michigan
SSP	System Security Plan
TAR	Technology Assisted Review
WCAG	Web Content Accessibility Guidelines
VPAT	Voluntary Product Accessibility Template

2. BACKGROUND

The Michigan Attorney General (AG) is the lawyer for the State of Michigan. The AG is a full-service law firm, handling files ranging from criminal prosecutions to government bonds, multistate antitrust litigation to environmental enforcement actions, and more. This Solution is for an eDiscovery system. The Contractor will provide software products and professional services to address the following aspects of the Electronic Discovery Reference Model (EDRM): (1) identification; (2) preservation; (3) collection; (4) processing (including predictive coding); (5) review; (6) analysis; (7) production; and (8) presentation. Also, audio and video file editing services will be provided.

3. PURPOSE

The State is for a *Contractor Hosted* Software Solution and applicable Services

Term of the Agreement: Three (3) year base contract with up to five (5) one-year renewal periods.

4. IT ENVIRONMENT RESPONSIBILITIES

Definitions:

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

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

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

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

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

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

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

Component Matrix	Identify contract components with contractor or subcontractor name(s), if applicable
Facilities	Contractor located at Brooklyn Park, MN and Austin, TX
Infrastructure	Located at Cloud Head Office: Microsoft Corporation One Microsoft Way, Redmond, Washington, USA
Platform	Relativity
Application	Relativity
Storage	Contractor located at Brooklyn Park, MN and Austin, TX
Backup	Contractor located at Brooklyn Park, MN and Austin, TX
Development	Contractor located in Austin, TX and Eden Prairie, MN

5. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

6. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
State Employee	Read, Write, Administrative	20	20

Contractors	Read Write	50	50
-------------	------------	----	----

Contractor Solution must meet the expected number of concurrent Users.

There are no limitations on the number of concurrent reviewers in any Contractor hosting location.

7. ACCESS CONTROL AND AUTHENTICATION

The Contractor’s solution must integrate with the State’s IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy (<https://www.milogintp.michigan.gov>), which consist of:

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

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

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

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

To integrate with the SOM MILogin solution, the Contractor’s solution must support SAML, or OAuth or OpenID interfaces for the SSO purposes.

SSO and SAML are both supported for Relativity. There are security parameters that need to be reviewed prior to using these authentication methods.

For Nebula Contractor uses MFA and does not currently support SSO. SSO support for Nebula is currently under development. Rollout is anticipated sometime in 2023.

8. DATA RETENTION AND REMOVAL

The State will need to retain all data for the entire length of the Contract unless otherwise directed by the State.

The State will need the ability to delete data, even data that may be stored off-line or in backups.

The State will need to retrieve data, even data that may be stored off-line or in backups.

Contractor will require written confirmation in order to fully delete a database, and a certificate of destruction will be provided upon request.

9. END USER AND IT OPERATING ENVIRONMENT

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

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

- Google Chrome
- Microsoft Edge
- Firefox
- Safari

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

10. SOFTWARE

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

Contractor must provide a list of any third party components, and open source component included with or used in connection with the deliverables defined within this

Contract. This information must be provided to the State on a quarterly basis and/or if a new third party or open source component is used in the performance of this Contract.

Look and Feel Standards

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

SOM IT Environment Access

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

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

Phase/Functionality	Solution Details
Identification	Nebula v22.09.00
Early Case Analytics (ECA)	Nebula v22.09.00
Litigation Hold Management	Nebula v22.09.00 Relativity Server 2022 (12.1.537.3)
Presentation	Nebula v22.09.00
Collection	Cellebrite Physical Analyzer v7.57 Logical Analyzer, Reader & UFED Cloud v. 7.55 Cellebrite Inspector (for Mac analysis v 10.6 EnCase v 8.11
Processing and Data Analytics	Nebula v22.09.00
Review	Nebula v22.09.00 Relativity Server 2022 (12.1.537.3)
Predictive Coding	Nebula v22.09.00 Relativity Server 2022 (12.1.537.3)
Production	Nebula v22.09.00 Relativity Server 2022 (12.1.537.3)

Presentation	Not applicable.
Transcript Management	Relativity Server 2022 (12.1.537.3)
Self Service Model	Nebula v22.09.00

Contractor will maintain an entire department dedicated to supporting Relativity. Contractor’s TechQ team will be staffed 24x7.

Contractor’s SaaS solutions operate using a standard web browser, secured with Secure Sockets Layer (SSL), and do not require the separate installation of additional hardware and software by the State. Contractor will provide the support and information required to ensure the State’s access to the platform. If connection via WAN is desired, WAN traffic utilizes an MPLS network and it is segmented from both Internet traffic and the server subnets.

For matters hosted in Relativity, the State can use the Relativity Analytics as well as Contractor’s proprietary Analytics package which is built directly into the platform. Analytics include; Contractor’s Predictive Coding, Workflow, Natural Language Processing, Email Threading, Near-Duplicate Detection and Language Identification. The analytics are outlined in detail below and are available in Relativity (Natural Language Processing only available in Nebula) and proprietary platforms.

Nebula is Contractor’s proprietary next-generation platform for unified Information Governance, Legal Hold, and end-to-end eDiscovery.

Nebula is an end-to-end eDiscovery solution that will help the State find smarter ways to cull, process, review and manage documents while creating substantial time and cost savings –in an application that is easy to use, modern, sleek, and intuitive. Nebula will allow the State to filter data, on the fly, while seeing how the search terms are hitting on the data in real-time. The State will not just receive a report with the number of hits. Instead, the State will see the actual document with the hits, evaluate the context and immediately fine-tune the search or filtering parameters on the fly.

Nebula offers in-depth deep dive search capabilities and detailed reporting. The platform comes with built-in data analytics including Contractor’s proprietary Predictive Coding, email threading and near-duplicate identification, along with Contractor’s proprietary review accelerator applications.

Contractor can handle all data collection, data processing activities and loading to either Nebula or Relativity and data will be hosted in secure data centers. Otherwise, contractor will provide authorized users with access and support users on an as-needed basis.

Nebula Workflow™ will automate document distribution and reviewer coding validation to maximize efficiency, accuracy, and defensibility.

“Firm Administration” will allow the State’s case teams to have full control over:

- New Repository creation and associated Matter management
- User account creation and maintenance
- User Group creation, membership, and assignments
- Permission Templates for easy cloning of permission sets across separate User Groups firms, corporations, and agencies alike.

Nebula’s User Management, the administrative feature controls user access and authentication within the Nebula platform.

Each user is assigned to a “Firm” (e.g., organization), with select users from each Firm being used to construct well-defined user groups. User group “Assignments” then control which projects those user groups can access. Within each Assignment, administrative users can fine-tune feature access from a completely redesigned permissions UI.

Permission templates for rapid reusability of custom roles, the ability to copy one or several user group attributes to expedite setup of related user groups, and “Firm Administration” capabilities that will allow the State to self-manage its own users, groups, assignments, and projects.

The State will have access to a fast and responsive review platform. Review in Relativity or Nebula is straightforward, and Contractor will provide training for all users at the onset of the matter. The State’s administrators (or designated users) will have full access to control the review environment.

- **KLDiscovery Predictive Coding** leverages machine learning to categorize and prioritize documents in real time via Continuous Active Learning (CAL). Continuous Active Learning may be used on all matters as a review aide; no special seed set or prep work is needed for the State to opt to run CAL on every matter. Documents that are most likely to be responsive will be queued up for review first. If CAL is used with the automated workflow process, the batches will be automatically updated to include the documents that are most likely to be responsive. Doing this will

allow the State to get a handle on its matter sooner, to understand the universe of favorable / unfavorable documents and yield significant results in terms of case strategy, including settlement discussions.

- **Workflow** automates review management with systematic processes for document distribution, check-in and quality control. The dynamic batching process means no manually creating static batches of documents throughout the review process. Workflow can be customized to batch certain types of data for the applicable reviewers (e.g. language, IT based, financial). CAL can be incorporated therein to prioritize batching and reduce volume of review as desired, and an additional layer of QC with respect to discrepancy between manual review and CAL rankings.
- **AutoRedaction** will greatly reduce the burden of the redaction process by automatically finding and redacting PII and other sensitive information from documents in a workspace, resulting in faster, cheaper, and more reliable redactions that are audited and easy to identify for quality control purposes.
- **Award-Winning A/V Suite** allows users to review multimedia and redact audio files directly inside the review platform.
- **PrivLog Builder** automatically generates privilege log data directly from the review tools and will give users the ability to standardize names across the entire population without the manual process. Templates can be saved for use across matters.
- **Native Spreadsheet Redaction** will allow reviewers to redact content from within Excel files without the need to convert to tiff image. Options for redactions include removal of rows, columns, worksheets, formulas, cells and standard text redactions. Pristine copies of the original file are always maintained.
- **Natural Language Processing** (included in Nebula only) allows for advanced concept searching and clustering. In addition to clustering, NLP offers sentiment analysis which is the ability to analyze and detect the feeling of an email or message. The tool will review and score segments of messages. Nebula will use this information to allow searching and filtering of documents based on the scores. Using this information, users can find documents that might have a negative feel or filter out documents that have only a positive feeling. Additionally, entity detection will allow Nebula to detect, group and show proper names, businesses, locations, currency, and other categories. Nebula will allow filtering by categories or even specific values within categories. Users will be able to see what the most common values are within each

- category as well.
- **Email Threading:** will allow users to group emails by conversation and view where in time a particular email occurs in the conversation using a visual flag. Also indicates which emails in the group have unique content and which are completely duplicative to help streamline the review and assist with coding consistency. When performing a search users may also retrieve email thread members, providing users with additional context for search results.
 - **Near-Duplicate Detection:** will allow users to identify and easily retrieve all duplicates and near duplicates of any document in the dataset post processing as well as compare two near duplicate documents side-by-side to see the differences.
 - **Language Identification:** will provides users with information regarding what languages are present in each document set, allowing users to search and identify grouping of documents in different languages.

Contractor offers two ECA platforms - Relativity and Nebula. In both platforms, the State will have access to text and metadata to perform all ECA functionality in a reduced hosting footprint. For Nebula, Live filtering is built into the platform which provides real-time results based on the dynamic search options available.

The Natural Language Processing (“NLP”) tool is available at no cost to the State in ECA and review. This tool allows for clustering and advanced concept searching. In addition to clustering, NLP also offers sentiment analysis which is the ability to analyze and detect the feeling of an email or message (positive vs negative). This information is searchable and allows for documents to be filtered based on the sentiment scores / values. Using this information, users can find documents that might have a negative feel or filter out documents that have only a positive feeling. The tool will review and score segments of messages. This provides real-time access to results which can also guide additional searches, resulting in lower promotion costs and reduced active review and hosting costs.

Entity Detection will detect, group and show proper names, businesses, locations, currency, and other categories. This information may be filtered by categories or even specific values within categories (i.e., filtering to show all colors vs only “blue”). Users will be able to see what the most common values are within each category as well. The State can seamlessly promote the results of ECA to review in Relativity or Nebula.

Mitrastech LegalHold is Contractor’s SaaS solution for end-to-end management of the legal hold process, enabling both defensible mitigation of litigation risk and improved outcomes. Additional key features and capabilities include:

- Comprehensive and flexible templating system

- Management of custodian communications and compliance, including automated reminders and escalations
- Collection workflows/processes
- Analytics and Reporting, including custom reporting
- Integration capabilities with Active Directory, matter management, and HR solutions

Nebula Archive connects to data at the source and copies it to the Archive for preservation. Automated validation checks ensure the data is captured accurately and comprehensive logging supports chain of custody. Data stored in the archive cannot be altered or deleted except when the matter is completed.

Contractor's team will deploy, usually within 24-48 hours, to perform on-site or remote collections. The team can collect data from cloud-based and web-based services (such as SFTP) directly from Contractor's secure labs.

Contractor does not outsource collections, forensic analysis or imaging work. All work will be performed by Contractor's full-time employees, all of whom are certified and have extensive experience supporting clients via affidavits, certifications and deposition and trial testimony.

The team is experienced in collecting from various environments including automobiles, boats, and has used Contractor's RCMgr tool to collect data from within war zones.

Contractor will perform MS Teams and Slack collections with follow on processing for review. Contractor will collect the contents of each Team channel as well as the general chat messaging. Attachments to Teams chat messages will be collected from the appropriate SharePoint locations and associated with the chat message.

The team will handle sensitive collections, cultural differences and respond to concerns the State may have when having a personal device imaged. Contractor will schedule collections so that they do not interfere with the State's ongoing business.

Contractor's remote collection tool, RCMgr is also available to the State if performing collections internally or with the support of DTMB's IT teams. Contractor's Remote Collection Manager (RCMgr®) kit allows for the imaging of laptops and desktops, targeted imaging from drives or network shares, and will pull custodian mailboxes and/or full EDBs from Exchange servers. The software enables fully defensible custodian self-collection. Contractor would pre-load the custom software to an external drive and deploy the drives to any client location on short notice. Once received, the drive is plugged into the device to be collected, security prompts are answered, and the imaging process will run. Once complete, the RCMgr® drive will be shipped back to Contractor's laboratories for verification and hashing. The software is SQL based and Contractor will testify to its processes.

Contractor will rely on proprietary Cloud-Based collection technology as well as third party forensic software specific to Cloud content. Contractor has the ability to collect cloud-based acquisitions related, but not limited to, Dropbox, Box.com, GSuite/Drive, iCloud, Slack, Jira, HipChat, Confluence, O365, AWS, Azure, and Zendesk. Contractor has forensic developers that focus specifically on developing custom acquisition and conversion tools for cloud-based and collaboration-based technologies.

The technology supports automated data capture through Connectors from dozens of systems, including Exchange Online, OneDrive for Business, SharePoint Online, Teams, and more.

Contractor supports more than 7,000 file types. Any processed file with extracted or OCR text and/or available metadata, is searchable within the platforms. Documents such as photos or other "image" files that do not contain text would only be searchable based on the available metadata.

Contractor's Advisory Services team and project managers will work consultatively and collaboratively with the State to proactively understand the needs of each matter and to provide guidance regarding efficient and defensible identification, preservation and collection strategies. Contractor's Advisory Services consultants will work with the State to draft ESI Protocols and prepare for Meet & Confer sessions. Contractor's technology stack will enable Contractor to assist the State in gaining early insight into data that provides a more holistic perspective into the larger discovery process. This early data/early case assessment (EDA/ECA) process will be accomplished through a combination of technologies and collaborative consultation including through Nebula's transparent ECA and Natural Language Processing, which will allow users to view documents in real time while Search and Analytics are applied in ECA.

Contractor will work with the State to define and implement a defensible data analysis or early data assessment protocol that will include search strategy and analysis, keyword analysis, and data culling strategies to ensure that the right documents are promoted for full review, while irrelevant documents are culled from the potential review population. This process will leverage available technology, the State's knowledge of the matter, and Contractor's expertise, to craft efficient and defensible strategies that will result in decreasing the size of the review set and, ultimately, saving time and money in the review stage.

The use of advanced data analytics technologies is used to audit within the applications in which the work is performed:

- Creation and evaluation of data maps to provide targeted source data collection.
- Analysis of data ingestion and de-duplication reports to cull by data type, custodian, date, and file path information.
- Metadata index creation.
- Creation of term dictionary, separated by parts of speech.

- Development of custom searches to identify most relevant documents and promote for review by:
 - Eliminating the least relevant documents.
 - Identifying potentially relevant privilege documents.
 - Grouping documents by most relevant issue(s).

Documents requiring redactions can be fed to the first pass review team with quality control performed by the privilege or second pass team. Alternatively, the privilege team can apply all redactions required. Contractor will work with the State to determine a preferred workflow for each matter.

The AutoRedaction application will locate and redact sensitive information such as Social Security Numbers, tax ID numbers, bank account numbers, credit card information, and other data with specific patterns. Through a completely audited process, redaction will be applied to the image and any discrepancies between extracted text and OCR performed by the application are flagged for manual review.

Finally, the A/V Suite will simplify the review of multimedia files within any of the review tools. This application allows reviewers to visualize audio files and have total playback control directly in the review application without the need for third party software. Reviewers can also easily redact and produce audio files directly in the review platform. Unaltered copies of the files are always maintained.

The Predictive Coding (“Nebula AI”) application will be used to identify relevant documents. The system compares and contrasts relevant and irrelevant documents trained while building its model and suggests “focus” documents to train based on this contrast. For example, one may have coded a “black” document as relevant and a “white” document as irrelevant; the system would provide various “gray” documents to further define what is relevant, improving the overall model.

Documents are scored on a scale of 0-1 (as a percentage); the higher the score, the more likely relevant.

Reporting will provide a breakdown of how many documents are escalating to various scores and the distribution of documents at various levels. If a control set is completed, additional statistics such as prevalence, recall, precision and accuracy can also be provided.

Review platforms are accessed using a standard web browser via a secure TLS connection on port 443. No software will be installed on the State’s computers or workstations.

Contractor’s tools are completely Unicode compliant. The processing tools will support virtually all languages including CJK. Contractor can run language detection either

during processing or once the data is in the review tool; foreign language detection and identification has been included in the State of Michigan's processing rate at no additional cost. The Language Identification application will analyze the text of documents and recognize a primary and a secondary language. Documents can be batched out to the proper review teams automatically using the Workflow application. If needed, machine translation is also available as an additional option.

11. INTEGRATION

The State does not require any Integration services at this time.

12. MIGRATION

The State does not anticipate any Data Migration services at this time.

Cases currently hosted with a vendor will remain with that vendor while the file is active so as not to disrupt pending litigation. Although there may be a few exceptions, generally only new cases will be assigned to the Contractor. If, however, the Contractor is assigned a case currently hosted by another vendor, the Contractor must assist in transitioning or migrating data as requested by the State.

13. TRAINING SERVICES

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

Contractor must offer onsite, webinar, and telephone training for power users, attorneys, and support staff.

Contractor should provide an annual training session about Contractor's available services and e-discovery tips, trends, and updates.

Contractor should provide power user or administrator certifications available/offered.

Contractor has a dedicated training team to support the State. Contractor has a dedicated Technology Group to support the State's use of the analytics platforms. The team will support the State through all aspects of utilizing analytics workflows.

The training strategy will be need based. Contractor's team will train not only on the technology, but on the workflows established to ensure consistency. Beyond the initial training session, additional training is available to all users upon request. Contractor has a group of dedicated trainers who are available to handle requests for additional or specialized training sessions as they arise/on short notice.

During all training sessions, Contractor will cover the tools and functionality that the State team feels would be of most use. Once the State's team is comfortable with all regular functionality, advanced training in other areas of interest to include analytics, assisted review, etc. will be added. For end user training sessions, Contractor will utilize the State's database in to cover any questions. The subject matter covered will be tailored in advance to be appropriate to the users in attendance. Review teams will receive instruction in tasks such as basic platform navigation, retrieving and turning in assignments, and coding and reviewing documents.

Administrator level training will be designed based on the desires of the State and the length of time required will vary.

All training will be on-demand and on an as-needed basis. Training will be offered via a live Teams meeting. These sessions will last approximately 1-hour with additional time if needed. These sessions can also be recorded for future use upon request. Trainings can also be offered in person, if appropriate.

Once training is complete, materials will be provided during the initial training that will be provided to the State and their outside counsel as well as a link to the online help site. Contractor also offers a robust video training library that is accessible on demand to authorized users.

All end-user training will be provided at no cost.

Formal certification training is offered through the Nebula Certification course, known as Nebula Academy, will be offered at no cost to the State. Contractor will offer a new Reviewer level course and Administrator course. Upon each course completion, attendees may take an online test to obtain their Nebula Certification.

Beyond matter-specific training offered at the start of each project, Contractor will share knowledge and expertise that can support and advance the goals of the State. This can come in the form of individualized training and/or thought leadership that focuses on either technical/process best practices or industry trends (i.e., TAR/Predictive Coding, ECA Strategies and Efficiencies, etc.).

The State will receive detailed instructions and training materials, as well as help sites and access to Contractor's training team for full support.

All Nebula training materials are hosted online at NebulaHelp.ediscovery.com

14. TRANSITION RESPONSIBILITIES

See Schedule G – Transition In and Out Plan

15. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

Contractor must develop and submit for State approval complete, accurate, and timely Solution documentation to support all users, and will update any discrepancies, or errors through the life of the contract.

The Contractor’s user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests. All necessary documentation will be provided.

16. ADDITIONAL PRODUCTS AND SERVICES

17. CONTRACTOR PERSONNEL

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

Contractor
Name: Jay Horowitz Address: 9023 Columbine Road Eden Prairie, MN 55347 Phone: 1 917-751-9796 Email: Jay.Horowitz@KLDDiscovery.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
Name: Jason Davison Address: 9023 Columbine Road Eden Prairie, MN 55347 Phone: 571-388-6511 Email: Jason.Davison@KLDDiscovery.com

18. CONTRACTOR KEY PERSONNEL

Contractor Account Manager/Representative. 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 services, matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
Name: Jay Horowitz
Address: 9023 Columbine Road Eden Prairie, MN 55347
Phone: 1 917-751-9796
Email: Jay.Horowitz@KLDDiscovery.com

19. CONTRACTOR PERSONNEL REQUIREMENTS

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

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

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

On-Site Work. Contractor’s personnel will be required to sign-in and wear State issued identification badges while inside any State facility

Offshore Resources. Due to the sensitive nature of the data in this solution, offshore resources are not allowed.

Disclosure of Subcontractors. Contractor intends to utilize the following subcontractors:

- Microsoft for purposes of hosting Nebula via Azure. Microsoft is a key provider of the infrastructure hardware and a strategic partner in the joint development of other connectors for the Office 365 and Exchange 365 environments.
- Relativity.
- Kensium is used for Scanning and Coding in the US.

20. STATE RESOURCES/RESPONSIBILITIES

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

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

State Contract Administrator
Name: Marisha Curtis
Phone: 517-328-9462
Email: curtism16@michigan.gov

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

DTMB Program Manager
Name: Michael Weiszbrod
Phone: 517-242-1272
Email: weiszbrod@michigan.gov

Agency Program Manager
Name: Dustin Senneker
Phone: 517-335-7573
Email: sennekerd@michigan.gov

21. MEETINGS

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

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

- System Security Plan (SSP) and related Security Meetings

Software Configuration meetings

Members of Contractor's Information Security, Information Technology or other relevant teams will be available to attend Security Meetings and Software Configuration Meetings held via video-conference, telephone-conference or in-person as required (video or telephone conference meetings preferred).

22. PROJECT CONTROL & REPORTS

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

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

Reports will be provided by email in a spreadsheet format and can be provided at the frequency of the requirement of State based on the reporting requirements provided. This is not a real-time report; generated for use by the State based upon historical data.

Monthly reporting is provided showing a high-level overview of the data across the State's matters, a breakdown of users and activity, and additional metrics upon the request of the State such as responsiveness rate, data analytics results, cost summaries, etc. Reporting is available for each phase of an individual matter. Upon initial receipt, a report is generated indicating the amount of data received, custodians included, and initial document counts. During processing, reports are generated providing details on filtering results, deduplication results, and exceptions encountered. Reports that are generated within the review platforms include Reviewer Statistics and Production reports and can be accessed on demand by the State.

Reports will also be generated and provided throughout the managed review process. While all workflows and reports are customizable, the standard workflows include

regular reporting on metrics such as review progress, reviewer productivity, quality control, and costs. The Reviewer Progress Summary report is used to determine how well the State's review team is progressing on an individual basis. The report details how long users have been logged into the platform, as well as how many documents and pages have cumulatively been categorized. Also, the review platforms offer document audit histories and robust reporting capabilities that allow for the creation of numerous customized reports to analyze user activity. Additional reporting services can include, but are not limited to,

- Privilege review/logging
- Redactions
- Key document reporting
- Timelines
- Other information as requested on a specific matter

Contractor will frequently use technology assisted review and analytics in managed reviews to assist with the productivity and quality control process. Contractor will generate reports related to TAR, CAL, and the use of analytics as needed.

In addition, the State will have access to the Client Portal which is available at no additional charge. This knowledge repository is accessible anywhere in the world – including on mobile devices and allows viewing of all critical case metrics, project details, and matter documentation. The State will immediately have access to the following:

Case Information

Dashboards of bibliographic information displayed for each matter, including case caption, client and law firm details, Contractor contacts, start date, matter status, and any regional restrictions.

File Library

Organize and share case documentation – such as production specifications, search reports, review protocols, agreements, and collection logs – into customized folders for instant availability and improved file management. Documents are organized at the matter level, and administrators can grant matter-specific access to users.

The Client Portal incorporates these additional features:

- Real-time tracking and visibility into metrics and progress updates on active projects
- Documentation for historical matters with granular, in-depth project statistics
- Consolidated reporting for portfolio intelligence, allowing the roll-up of data across matters
- Customizable layouts, tables and dashboards tailored to each user's unique needs

23. PROJECT MANAGEMENT

The Contractor Project Manager will be responsible for maintaining a project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources – both Contractor and State - required to meet the timeframes as agreed to by both parties.

Changes to scope, schedule or cost must be addressed through a formal change request process with the State and the Contractor to ensure understanding, agreement and approval of authorized parties to the change and clearly identify the impact to the overall project.

SUITE Documentation

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

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

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

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

Contractor's teams can accommodate and meet the requirements of the PMM/SEM structure. The SUITE templates provided will suffice; Contractor will not submit other documents to be used in place of the templates provided by the State of Michigan. In order to meet all requirements, and in an effort to complete all required document submissions in a timely manner, several representatives from the Contractor team will

be utilized for these submissions including: Billing, Business Development, Project Management, Data Hosting and Application Support, and Information Security.

Milestones/Deliverables for Implementation

The milestone schedule and associated deliverables are set forth below.

Milestone Event	Associated Milestone Deliverable(s)	Schedule
Project Planning	Project Kickoff	Contract Execution, SSP Initiation + 10 calendar days
Requirements and Design Validation	Validation sessions, Final Requirement Validation Document, Final Design Document, Final Implementation Document, SSP Related Tasks and Responses	Execution + 90 calendar days
Provision environments	Validate Test and Production environments	Execution + 90 calendar days
Installation and Configuration of software	Final Solution and Testing Document	Execution + 120 calendar days
Testing and Acceptance	Final Test Results Report, Final Training Documentation, Final Acceptance, SSP Completion, SOM Authority To Operate (ATO) Approvals	Execution+150 calendar days
Post Production Warranty	Included in the cost of Solution.	Production + 90 calendar days
Production Support Services	Ongoing after Final Acceptance.	Ongoing

24. RESERVED

25. ADDITIONAL INFORMATION

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

SCHEDULE A – TABLE 1 – BUSINESS SPECIFICATION WORKSHEET

A	B
Business Specification Number	Business Specification
REQUIRED	
	Identification
1.0	System will provide search and identification capabilities for Office 365 (Outlook, OneDrive, Teams, SharePoint).
2.0	System will ingest for Microsoft Office 365 and email attachments.
3.0	System will support average processing speeds of at least 20 GB per hour. Data Volume Low/High Processing Timelines: 0-50 GB <= 24 Hours 51-250 GB 24-36 Hours 251 – 500 GB 36 – 48 Hours 501 - 1000 GB 48 – 96 Hours
4.0	System will provide search and identification capabilities for backup tapes or other archival storage media.

A	B
Business Specification Number	Business Specification
5.0	<p>System will provide search and identification capabilities for network share locations, desktop share drives, laptops, tablets, and cell phones.</p> <p>Contractor has the ability to use the Remote Collection Manager (RCMgr) solution. RCMgr is an external hard drive that contains the self-developed forensic collection application. Contractor will send RCMgr to the State's IT personnel for collection from servers.</p> <p>When collecting from desktop or laptop devices, Contractor can send RCMgr drives directly to either IT support or the device users themselves. RCMgr can be used to create full forensic images of laptops, desktops, and servers, or perform targeted, hash-verified collections. It comes with a single page of plain-English instruction, making it easy to understand and deploy by even non-tech-savvy end users. Additionally, for web- and cloud-based applications as well as for mobile devices backed up to the cloud, Contractor can collect data remotely from Contractor's secure labs saving the time and expense of traveling on-site.</p>
6.0	System will provide search and identification capabilities for IRMA (Alchemy Software), HP TRIM, HP Content Manager and FileNet.
7.0	System will provide search and identification capabilities for databases, including Microsoft SQL and Oracle.
8.0	System will provide file type support for Adobe Acrobat PDF (most current version).
9.0	System will provide tools to decrypt Microsoft Office documents, PDF files, or other files that may be encrypted.
10.0	System will support reporting on encrypted and protected files.

A	B
Business Specification Number	Business Specification
11.0	System will support File type for ASCII Text.
12.0	System will support file type for Microsoft Access, Excel, PowerPoint, and Word from 1997 through 2013.
13.0	System will support file type for Microsoft Word for DOS all versions.
14.0	System will support file type for Microsoft RTF.
15.0	System will support file type for FileMaker Pro version 6.0 v4.
16.0	System will support file type for HTML.
17.0	<p>System will support file type for audio files (such as WAV, MP3, MP4, WMA, MOV), including redaction of audio files directly within the platform or in a completely audited manner as well.</p> <p>Along with this, the solution will allow users to visualize audio files, and have total playback control.</p>
18.0	System will support file type for video files (such as MPG, MP4, AVI).
19.0	System will support file type for ZIPs and other container files.
20.0	System will support file type for image files (such as TIFF, JPEG, PNG and GIF).
21.0	System will support file type for OCR of image files in TXT and PDF file format during data processing and at the other end of the eDiscovery lifecycle.
22.0	System will support file type for SMS or other text messaging types.
23.0	System will support for the inclusion or exclusion of system file types.

A	B
Business Specification Number	Business Specification
24.0	System will provide capability to account for name changes, aliases, and different naming conventions that may relate to the custodians being searched.
	Early Case Analytics (ECA)
25.0	System will have ability to ingest, filter, including global deduplication, and search data of varying types.
26.0	System will have ability to load text only files into a database for evaluation.
27.0	System will have ability to cull or filter out unnecessary data, such as NIST files, junk email, mass mailing lists, or other non-business related data.
28.0	System will provide support for major social media such as YouTube, Facebook, Twitter, Instagram.
	Collection
29.0	System will allow encryption provided for any data being transmitted to and from the hosting center.
	Processing and Data Analytics
30.0	System will have ability to OCR images and extract text from native documents.
31.0	System will have ability to process a forensic copy of a hard drive (e.g., AFF, AFF4, E01, L01, etc.)
32.0	System will have ability to import load files of images, native files, OCR or extracted text from other software programs.
33.0	System will have ability to recognize hash values or other metadata to de-duplicate.

A	B
Business Specification Number	Business Specification
34.0	System will provide statistical and graphical analysis reporting of collected data based on custodian, date range, and file type prior to processing.
35.0	System will have ability to filter collected data by custodian, date, file type, and file size prior to processing.
36.0	System will have ability to filter data by NSRL (National Software Reference Library) database list (de-NIST) prior to or during processing.
37.0	System will have ability to filter collected data by customer-defined known file lists prior to processing.
38.0	System will have ability to de-duplicate records and data of a single custodian across multiple data stores and across all custodians.
39.0	System will have ability to maintain family file relationship structures.
40.0	System will support processing content containing international languages (Unicode). Please detail the languages that are and are not supported.
41.0	System will support processing exception reports to understand file errors, warnings, and key processing metrics such as de-duplication rates, total # of messages and loose files, and average document size.
42.0	System will support extraction of attachments from emails and ability to process attachments as separate documents that are associated with the original email message. System maintains metadata between original files and attachments.
43.0	System will provide capability for metadata extraction making it available for review.
44.0	System will have ability to later add information to an index without re-indexing the entire case dataset.

A	B
Business Specification Number	Business Specification
45.0	System will support processing of nested email attachments (e.g., the solution can process all documents included in an email which contains one or more .msg attachment and their attachments, which may include a ZIP file attachment or loose Word or Excel documents).
46.0	System will support extraction and processing of files within container files such as ZIP and RAR and support the processing of files in nested containers (e.g., a ZIP within a ZIP within a ZIP).
47.0	System will have ability to identify and report on encrypted and password protected files.
48.0	System will support wildcards and proximity searching.
49.0	System will support OCR fuzzy searching or other methods of searching OCR, including: dtSearch (Boolean, proximity, stemming, fuzzy, & wildcards), field-based searching, redaction location, predictive coding, concept searching (through analytics), language-based analytics, and the ability to combine all of the above into custom saved searches, with optimum results.
50.0	System will support stemming and literal searches.
51.0	System will support search of content in tags or document notations.
52.0	System will support search on international content (Unicode) either during processing or once the data is in the review tool, and analyze the text of documents and recognize a primary and a secondary language.
53.0	System will support searches by document ID, source location, custodian or processing batch.
54.0 T	System will support search by senders, recipients, urgency, and direction (e.g., internal email only) of email.
55.0	System will support search by attachment content or type.

A	B
Business Specification Number	Business Specification
56.0	System will support real-time and iterative sampling of search results, and the sampling must be able to be drawn from any subset of documents.
57.0	System will provide ability to visually track email threads for responses based on content and metadata, not just metadata, allow users to view where in time a particular email occurs in the conversation using a visual flag, indicate which emails in the group have unique content and which are completely duplicative. All emails on every State matter are to be threaded with no additional cost to the State, along with access to Natural Language Processing in Nebula.
58.0	System will have ability to identify and group documents based on language, and data that is in foreign languages must be directly routed to reviewers who speak that language.
59.0	System will have ability to organize and group related loose files and custodians for analysis, either organized as search results or collected as Lists.
60.0	System will provide hit highlighting in native documents, extracted text, metadata, and OCR.
61.0	System will cull-down and filter: Ability to filter documents across the entire case by sender or recipient domain, group, name, document type, custodian, and language type and display exact hit counts across the entire search result set for every filter.
62.0	System will have ability to ingest ESI received by the AG into a database for review by the State litigation team if necessary, regardless of the platform in which the ESI is produced.
63.0	System will have ability to establish secure file transfer protocol (SFTP) sites for the transfer of data, and data in transit must be encrypted using 256-bit encryption provided by TLS 1.2 or greater.

A	B
Business Specification Number	Business Specification
	<p>Data sent from Contractor to the State or other parties per State instructions, Contractor must encrypt the deliverables and use the Globalscape File Transfer Appliance.</p> <p>Where applicable, data at rest must be encrypted using AES256 at the hardware level.</p> <p>All physical media collected and prepared by Contractor must be encrypted, with the specific method of encryption dependent upon the software employed.</p>
	Review
64.0	<p>System will have ability to divide or batch out records so each reviewer is assigned a specific range or percentage of records, or by the source or significance of a subset of records; batches would include family members and ability to batch tag records.</p> <p>If CAL is used with the automated workflow process, the batches must be automatically updated to include the documents that are most likely to be responsive.</p>
65.0	System will have ability to easily organize documents intended for review into access controlled areas.
66.0	System will have ability to customize fields, tags, issue codes, and tagging permissions, and support an unlimited number of issue tags.
67.0	System will provide the ability to customize a template for use in new matter creation such as, but not limited to, review templates, database templates, production specifications, billing requirements, custom report requests, communication protocols, etc.
68.0	System will have ability to provide persistent highlighting on documents.

A	B
Business Specification Number	Business Specification
69.0	System will provide support for hierarchical tagging structures that define and require sub-tags based on parent tags.
70.0	System will provide ability for individual and bulk categorization and tagging.
71.0	System will support for tagging or classification of documents via a single mouse click.
72.0	System will support for HTML preview (or near native viewer) of all documents.
73.0	System will support annotation that is supported directly in the review user interface for all document formats.
74.0	System will support for hit highlighting of searched terms during review in native viewer or HTML preview.
75.0	System will support for user-friendly redaction of text, areas within a document, and entire pages; the ability to select the color of redaction, to overlay words within the redaction, and for the user to mouse over the redaction in transparency to see the words underneath; provide ability to burn in redaction for production.
76.0	System will provide find-and-redact functionality; the ability to batch-redact multiple pages; the ability to batch-redact PPI, PII, PHI, etc in a document.
77.0	System will provide reporting for reviewer progress and productivity analysis for each reviewer, along with reviewer actions, such as login, logout, search, tag, print, and export.
78.0	System will provide tools to delete or remove documents from the database pursuant to clawback agreements.
79.0	System will provide SFTP site for uploading and downloading documents.
80.0	System will be compatible with dual-monitor display.

A	B
Business Specification Number	Business Specification
	Predictive Coding
81.0	<p>System will provide technology/computer assisted review (TAR/CAR) capabilities (a/k/a predictive coding) in the software build such as:</p> <ul style="list-style-type: none"> • Workflow - Total control over all document batching with a dynamic Workflow system. • Predictive Coding • Natural Language Processing (NLP) • Native Spreadsheet Redactions – <ul style="list-style-type: none"> ○ Allows reviewers to redact content from within Excel files without the need to convert to TIFF images. • Auto-Redaction - Protect sensitive information and streamline the redaction process with an automated approach. • Email Threading - Group messages within an email chain to identify the most comprehensive versions of emails and navigate conversations. • Language Identification - Support multi-lingual data and increase review efficiency by automatically identifying the primary language on all documents in the State’s data set. • Near-Duplicate Detection - Automatically group textually-similar documents together, allowing for faster review of large amounts of records.

A	B
Business Specification Number	Business Specification
	<ul style="list-style-type: none"> • AV-Suite - Allows users to easily redact and produce audio files. • Workflow Reporting Suite - Provides dynamic, on-demand information on the progress, productivity, and tagging trends for document review projects run within the Workflow system. • Machine Translation - Leverage advanced AI-based machine translation technology to get accurate and reliable translations of documents written in most languages used across the globe. <p>For matters hosted in Relativity, Contractor must also provide Relativity Analytics and Brainspace in addition to Contractor's proprietary analytics package.</p>
	Production
82.0	System will support for individual production sets and batch export.
83.0	System will provide support for export of fielded data including but not limited to standard image/native productions, image only, native only, PDF, and searchable PDF to CSV, dat/opt, and dii with custom fields.
84.0	System will provide support for image-based productions such as TIFF, PDF. Document lists must be able to be formatted and exported in Excel, PDF, or HTML formats.
85.0	<p>System will provide support for export to Relativity, Concordance, Summation file formats (Bidder should name others if applicable).</p> <p>Productions will be able to be made electronically via FTP, or shipped on encrypted media including hard drive, DVD/CD, etc. Document lists can be formatted and exported in Excel, PDF, or HTML formats.</p>

A	B
Business Specification Number	Business Specification
86.0	System will provide support for export to EDRM XML compatible formats.
87.0	System will provide support for producing documents one at a time or in batches.
88.0	System will have ability to organize production sets.
89.0	System will provide support for burned-in redactions in a production set, where text is secured from unauthorized display, search, and review.
90.0	System will provide support for production mark-up tools that will provide custom header, footer, and watermark labeling of documents in image-based production.
91.0	System will provide support for Bates stamping onto images in a production set; ability to track production set numbers for each rolling production.
	Training
92.0	System will provide quick tips and checklists to orient attorneys new to e-discovery on-demand and on an as-needed basis.
	Customer Service and Technical Support
93.0	System will provide remote support.
94.0	Contractor will provide a fully staffed toll-free telephone support, and an online helpdesk for Nebula.
95.0	System will be able to meet Service Levels contained in Schedule D – Service Level Agreement .
	Miscellaneous

A	B
Business Specification Number	Business Specification
96.0	System will be able to develop checklists and standardized statements of work to guide State agency employees in defining scope of services and determining project budget
97.0	<p>System will have ability to document chain of custody of data, including but limited to relevant information such as (1) a full description of the equipment/media; (2) date and time received; (3) where it came from and who sent it to Contractor; (4) where it is stored and (5) details regarding its disposition.</p> <p>The Chain of Custody will record the hash value (MD5 or SHA-1) of the entirety of the data set or forensic image as to strengthen the defensibility of the collected data, in compliance with the U.S. Federal Rules of Evidence 902(13) and 902(14).</p>
98.0	System will have ability for contractor to maintain and provide detailed metrics on State's use of e-discovery products and services during entire term of contract
	Self Service Model
99.0	System will support software that provides client the ability to create/administer/delete their own workspaces, and different levels of access that can be customized by security groups.
100.0	System will support software that provides client the ability to create/administer/delete users.
101.0	System will support software that provides the client the ability to administer user permissions.
102.0	System will support software that provides the client the ability to create/modify/delete user groups.

A	B
Business Specification Number	Business Specification
103.0	System will support software that provides the client the ability to process data.
104.0	System will support software that provides the client the ability to run productions.
105.0	System will support program that provides the client the ability to bulk ingest or export image and native documents from a workspace.
	Litigation Hold Management
106.0	System will provide legal hold notice templates, and the ability to create hold templates.
107.0	System will provide the ability to configure and/or edit legal hold notice templates.
108.0	System will have ability to email legal hold notices to key personnel using Microsoft Outlook.
109.0	System will have ability to include in legal hold notices interview questions to custodians and ability to generate reports from there.
110.0	System will have ability to customize legal hold schedules and reminders as needed or a portal for custodians and litigation support staff to view multiple legal holds across cases/agencies. In the alternative, legal hold reminders that can be consolidated for multiple cases.
111.0	System will email recipients, be able to transmit receipt and acknowledgment of legal hold notices with simple click or other simple means.
112.0	System will allow for legal holds to be responded to through mobile devices in an optimized manner.
113.0	System will allow for tracking of legal hold notice issuance, receipt, reminders, and releases.

A	B
Business Specification Number	Business Specification
114.0	System will allow for legal hold tool modifiable to meet needs of Freedom of Information Act coordinators.
115.0	System will have ability for legal hold tool modifiable to provide notification to agency managers when employee departs state government employment and data must be preserved and not wiped for redeployment of computer.
116.0	System will have secure capability for person acknowledging legal hold (i.e., person provides a password to acknowledge receipt of legal hold by correct custodian).
117.0	System will have legal holds retained so that historical data can be reported on through the system.
118.0	System will have ability to escalate legal hold notices to supervisors for non-compliant employees.
119.0	System will provide reporting capabilities on status of legal holds by issuer or recipient group, e.g., across a department or agency.
	Preservation
120.0	System will provide support for legal holds on Office 365 (Outlook, OneDrive, Teams, SharePoint) and archive database.
121.0	System will provide support for legal holds on file shares located on physical and virtual servers and SAN/NAS storage devices attached to State network.
122.0	System will provide support for legal holds on desktops and laptops attached to State network.
123.0	System will provide support for multiple searches used to place and remove holds per matter.
124.0	System will provide support for multiple legal holds on a record without need for copies.

A	B
Business Specification Number	Business Specification
125.0	System will provide support for ability to remove multiple legal holds on a record per matter.
126.0	System will provide support for controlled suspension of automatic deletion routines.
	Collection
127.0	System will facilitate collection of preserved records (legal holds) by the file types listed in the Identification section above.
128.0	System will support for collection of files from Lotus Notes email server and archive database.
129.0	System will support for collection of files from Microsoft Exchange email server and archive database.
130.0	System will support for collection of files from file shares located on servers and SAN/NAS storage devices attached to State network.
131.0	System will support for collection of files from desktops attached to State network, including collecting a forensic bit-by-bit copy of the desktop hard drive.
132.0	System will support for collection of files from laptops attached to State network, including collecting a forensic bit-by-bit copy of the laptop hard drive.
133.0	System will support for the collection of cell phone data, e.g., Apple iOS and Android. For Apple products only (iPhone, iPod, iPad), Contractor can create, or assist an end-user in generating an iTunes backup of the requested device and transfer the content to Contractor via SFTP transport.
134.0	System will support for collection of multiple searches to place records into a legally defensible, secured location for each matter.

A	B
Business Specification Number	Business Specification
135.0	System will support ability for collection to occur in such a way that government operations are not interrupted.
	Processing and Data Analytics
136.0	System will have ability to unitize and process paper into digital format.
137.0	System will have ability to process (extract text and metadata) from all file types specified in the Identification section above.
138.0	System will provide support for all analysis features to operate on and across the entire matter, including matters up to 10 million documents.
139.0	System will provide automatic documentation or reporting of executed searches and keyword variation selections.
140.0	System will have ability to preview search results prior to running searches to remove obvious false positives.
141.0	System will support for relevance ranking: Retrieved documents that most closely satisfy the query criteria should be listed or ranked above those that match less exactly. Ranking should place a higher priority on matches in a title or subject than on those in body text.
142.0	System will use of directory information such as names, email addresses, and department groupings to extend the values of certain metadata fields, such as message recipients, or create new metadata, such as departments creating or receiving content.
143.0	System will provide ability to visually analyze email sender or receiver clustering representing periods of high activity or periods of no activity and the email addresses involved in the cluster.

A	B
Business Specification Number	Business Specification
144.0	System will have ability to group documents and emails together that pertain to the same or similar topic (clustering).
145.0	System will have ability to identify and group documents by frequently found nouns or noun phrases.
	Review
146.0	System will allow privileged communication to be tagged and a privilege log to be created, edited, and produced
	Production
147.0	System will support to “un-duplicate” data by custodian on export.
	Customer Service and Technical Support
148.0	System will provide onsite support available in Lansing and Detroit
	Miscellaneous
149.0	System will have staff located in Michigan

SCHEDULE B – PRICING

Year 1			
State of Michigan 3 TB - 20 TB All-In Subscription			
Tier	Volume	Proposed Monthly	Burst Rate (Per GB)
Tier 1	Up to 3 TB	\$23,040	\$8.65
Tier 2	3 TB - 4 TB	\$29,286	\$8.25
Tier 3	4 TB - 5 TB	\$34,816	\$7.85
Tier 4	5 TB - 6 TB	\$39,936	\$7.50
Tier 5	6 TB - 7 TB	\$44,442	\$7.15
Tier 6	7 TB - 8 TB	\$48,742	\$6.85
Tier 7	10 TB	\$55,296	\$6.20
Tier 8	15 TB	\$74,496	\$5.60
Tier 9	20 TB	\$89,088	\$5.00
Year 2 (2.5% Discount from Year 1)			
State of Michigan 3 TB - 20 TB All-In Subscription			
Tier 1	Up to 3 TB	\$22,464	\$8.65
Tier 2	3 TB - 4 TB	\$28,555	\$8.25
Tier 3	4 TB - 5 TB	\$33,946	\$7.85
Tier 4	5 TB - 6 TB	\$38,938	\$7.50
Tier 5	6 TB - 7 TB	\$43,331	\$7.15
Tier 6	7 TB - 8 TB	\$47,524	\$6.85
Tier 7	10 TB	\$53,914	\$6.20
Tier 8	15 TB	\$72,634	\$5.60

Tier 9	20 TB	\$86,861	\$5.00
Year 3 (2.5% Discount from Year 2)			
State of Michigan 3 TB - 20 TB All-In Subscription			
Tier 1	Up to 3 TB	\$21,903	\$8.65
Tier 2	3 TB - 4 TB	\$27,842	\$8.25
Tier 3	4 TB - 5 TB	\$33,098	\$7.85
Tier 4	5 TB - 6 TB	\$37,965	\$7.50
Tier 5	6 TB - 7 TB	\$42,248	\$7.15
Tier 6	7 TB - 8 TB	\$46,336	\$6.85
Tier 7	10 TB	\$52,567	\$6.20
Tier 8	15 TB	\$70,819	\$5.60
Tier 9	20 TB	\$84,690	\$5.00

State of Michigan Subscription Includes:

The State of Michigan Subscription includes all processing, hosting and productions within the specified volume parameters. Threshold capacity is based on total active capacity of combined active Review and ECA volumes, plus Nearline volume which is calculated at 50% of its footprint. ECA volume is based on metadata, text and indices.

Note that Tiers 7, 8 and 9 are presented as exemplars of rates for higher data volumes.

Subscription capacity is re-usable, i.e. as data is retired, the State will open up capacity for re-use.

Volume within each tier to be billed at the designated fixed monthly rate for that tier.

Should the State exceed the threshold of the current tier in any given month, the State will have the option to moving to the next higher tier or pay the Per GB Burst Rate for any volume in excess of the tier threshold each month that the tier threshold is exceeded.

To support the State in efficiently managing data volumes and cost, the State will have the ability to "Right Size" the subscription three (3) times per year.
This "Right Sizing" will allow the State to move down to a lower tier should data volumes be reduced due to the closing/archiving of matters.

The State will be allocated network storage for processing and archiving at 3x the current tier hosted capacity

Tier 1: 9 TB
Tier 2: 12 TB
Tier 3: 15 TB
Tier 4: 18 TB
Tier 5: 21 TB
Tier 6: 24 TB
Tier 7: 30 TB
Tier 8: 45 TB
Tier 9: 60 TB

Should the Network Storage allocated volume be exceeded for the given Hosting Tier, overages will be invoiced at \$1.50/GB/Month

<p>The State of Michigan subscription includes unlimited Nebula users.</p> <p>Should the State elect to leverage Contractor’s instance of Relativity, Relativity Users will be invoiced at the A La Carte rate of \$75/user/month.</p>
<p>The State of Michigan subscription includes an allocation of 10 Professional Services hours per month. These hours may be used for any project management or technical support that the State may request.</p> <p>Should the State exceed the provided Professional Services allocation in a given month, the Excess Hours will be invoiced at the A La Carte rates of \$150/Hour for Project Management and \$150/Hour for Technical Support services.</p>
<p>Upon request, Contractor will provide additional tiers for higher or lower volume thresholds, monthly Professional Services hours and/or other Contractor services and technologies.</p>

Collections	Unit	USD	Notes
Forensic Data Collection	Hour	250.00	Forensic analyst time supporting onsite collection of computers, servers, mobile and external devices.
Remote Forensic Data Collection	Hour	250.00	Forensic analyst time supporting in lab collection of computers, servers, mobile and external devices. Also includes the collection of internet based data sources including O365, Social Media and webmail.

RMDC - Remote Mobile Device Collection	Unit	1,150.00	Remote collection services for mobile devices – includes device image, media, shipping both ways and 24 x 7 x 365 technical support.
RCMgr Self Collection Computer	Unit	450.00	Drives/remote collection kit - includes drive image, shipping both ways and 24 x 7 x 365 technical support.
RCMgr Self Collection Server	Unit	750.00	Drives/remote collection kit - includes drive image, shipping both ways and 24 x 7 x 365 technical support.
RCMgr Drive Decryption	Unit	200.00	Decryption fee for native delivery of data. This fee will be waived if data processed by KLDDiscovery.
Forensic Analysis	Hour	300.00	Computer Forensic services including forensic in-lab preservation, active and recoverable deleted file listings, active and recoverable deleted email listings, internet history, removable media identification, and deliverable creation.
Expert Testimony	Hour	450.00	Forensic Testimony Services including deposition and trial testimony and authoring expert reports and affidavits.
Travel Time	Hour	50%	Travel time charged at 50% of the hourly rate for the service provided. Not to exceed \$1,000 per travel day.
Travel Expense	Item	Cost	Travel related expenses such as hotel, transportation, and meals billed at actual cost.

Processing	Unit	USD	Notes
Standard ESI Processing	GB	55.00	Process data, including de-duplication, keyword searching, date filtering, file type filtering; includes identification and OCR of all non-full text documents.
Selective ESI Ingestion (IN)	GB	15.00	Ingest, de-duplicate, and index content for keyword, date, and other Boolean/advanced filtering techniques. Identification and OCR of all non-full text documents.
Selective ESI Processing (OUT)	GB	75.00	Process data responsive to the filters applied.
Structured Data Loading	Hour	150.00	Load preprocessed structured data to database.
ECA Hosting	Unit	USD	Notes
ECA Hosting - Relativity (text, metadata and indexes only)	GB Month	8.00	Includes access to processed data (text, metadata) in Early Case Assessment (ECA) within a KLD review platform, for keyword testing and selection of data for promotion to review. 3 user maximum in the ECA platform.
ECA Hosting - Nebula (text, metadata and indexes only)	GB Month	7.00	Includes access to processed data (text, metadata and indexes) in Early Case Assessment (ECA) within a KLD review platform, for keyword testing and selection of data for promotion to review. 3 user maximum in the ECA platform.

Hosting	Unit	USD	Notes
Active Hosting Relativity	GB Month	8.00	Includes database setup, text, native & image access to data in an active state within a KLDDiscovery review platform. Active hosting charges for a given month shall be based on the largest data count hosted at any given time during the calendar month being billed.
Nearline Relativity Hosting	GB Month	4.00	Includes storage with the ability to retrieve text, native & image data in a nearline state within a KLDDiscovery review platform. In order for the nearline hosting rate to take effect, data must remain in nearline status continuously for at least one (1) calendar month.
Active Hosting Nebula	GB Month	7.00	Includes database setup, text, native & image access to data in an active state within a KLDDiscovery review platform. Active hosting charges for a given month shall be based on the largest data count hosted at any given time during the calendar month being billed.
Nearline Hosting Nebula	GB Month	3.50	Includes storage with the ability to retrieve text, native & image data in a nearline state within a KLDDiscovery review platform. In order for the nearline hosting rate to take effect, data must remain in nearline status continuously for at least one (1) calendar month.
User Access Relativity	User Month	75.00	Monthly user fee for Relativity Review.
User Access Nebula	User Month	0.00	Monthly user fee for Nebula Review.

			All data and each user account will remain active until such time that KLDDiscovery is asked to terminate it. Hosting and User access charges are not pro-rated; therefore, requests to terminate an account must be made by close-of-business on the last business day of the month in order to avoid being billed for the following month.
Analytics	Unit	USD	Notes
KLDDiscovery Analytics	File	Waived	KLDDiscovery technology for advanced analytics, including predictive coding, workflow, message threading, near-duplicate detection.
Relativity Analytics	GB	55.00	Content Analyst technology and indexing for concept searching, clustering, email threading, near-duplicate detection, language identification, categorization, and Relativity Assisted Review predictive coding.
Brainspace	File	0.03 (Year 1)	Includes Conceptual Clustering, advanced machine learning, etc.
		0.015 (Year 2)	
KLD Machine Language Translation Service	Every 1 Million Characters	40.00	Machine translation of foreign language text.

Professional Services	Unit	USD	Notes
Project Management and Technical Support	Hour	\$150/hr complimentary 10 professional hours per month (aggregate)	Project Manager -Consultative and customized support including but not limited to transmittal and analysis of electronically stored information, customized processing solutions, document review workflow design, document production query design, and quality control customization. Tech Support - Billable operations. Includes but not limited to processing and loading of 3rd party data into KLDISCOVERY review platform, including customization of load files. Create custom load file production template or special handling for productions. Technical support for review platforms. Support time is rounded up to 6 minute increments. All hours incurred (including weekends & holidays) billed at standard flat rate .
Consulting Services	Hour	425.00	Consulting Services including but not limited to information governance, preservation and collections, discovery readiness, ESI stipulation, early data assessment, predictive coding and review strategy.
Advanced Analytics Consulting	Hour	295.00	Consulting on optimal utilization of TAR feature, search term/ECA consulting, and predictive coding and review workflow consulting.

Data Management	Unit	USD	Notes
Case Disposition	Workspace < 2 TB	450.00	Upon case completion, the workspace will be taken down and copied to an external HDD. Includes tech time, landing media, and shipment.
	Workspace > 2 TB	750.00	
Offline Archive Storage	< 250 GB Month	25.00	Monthly storage fee for an archived database.
	250 GB – 1 TB Month	50.00	
	> 1 TB Month	75.00	
Offline Restoration	< 250 GB	500.00	One-time fee to restore a database from archive to an active state.
	250 GB – 1 TB	1,500.00	
	> 1 TB	2,500.00	
Original Media Storage	Media Month After 6 Months	25.00	Monthly storage fee for client media. If data is processed into a KLDISCOVERY review platform the first 6 months are included.
Media Destruction Deletion	Media	50.00	Provide certificate of destruction for deletion of client data from KLDISCOVERY servers and archive tapes.
Media Delivery	Unit	USD	Notes
CD DVD	CD DVD	15.00	CD DVD media for deliverables.
Flash Drive	USB	75.00	USB Flash Drive media for deliverables.

Hard Drive	HDD	199.00	Hard Drive media for deliverables.
Padlock	HDD	299.00	Padlock Hard Drive media for deliverables.
Freight	Cost	Cost	Freight charges, including postage, ground couriers, FedEx, etc.

Pricing Document Review – Remote Review Services

US Based Reviews				
Tier	1L/2L/ Privilege Review	Team Lead/QC	Assistant Review Manager	Review Manager
Platinum	\$48 -\$50	\$65	\$95	\$195
Gold	\$45	\$65	\$75	\$195
Silver	\$39	\$55	\$65	\$125
Document Review Analysts (non-licensed reviewers)	\$35	\$45	\$95	\$195

Platinum

- Significant experience working on advanced review matters such as large second requests, Antitrust matters, Civil Investigative Demands, white collar criminal investigations and numerous types of litigation regarding the financial sector. Strong proficiency across various document review tools and software programs including those related to Project Management and quality control metrics.
- Expert understanding and proven track record working on first level review, quality control and privilege logging workflows.
- Possess firm understanding and demonstrated application of “review rhythm” AKA the ability to code large quantities of documents consistently and correctly based on the Review Protocol and/or following guidance from the lead supervising attorney.

- Primarily based out of major markets such as New York City and Washington, DC.
- Extensive document review experience (1-15+ years).

Gold

- Proven experience working on small, medium and large review Projects including product liability cases, internal corporate investigations, corporate mergers and standard litigation discovery requests.
- Proficient in all review platforms utilized by KLD including but not limited to: Nebula, Relativity, EDR.
- Firm grasp of necessary skills to perform first level review, second level privilege review (based on the Review Protocol and/or following guidance from the lead supervising attorney) and assist with quality control workflows.
- Demonstrated ability to understand Review Protocols and make quick, confident decisions to code a document (based on the Review Protocol and/or following guidance from the lead supervising attorney).
- Aware of how each individual document reviewer fits into overall Electronic Discovery Reference Model (EDRM).
- Candidates based out of primary review markets including Chicago, DC Metro region and Eden Prairie.
- Prior document review experience (6 months – 3+ years).

Silver

- Competent document reviewers who possess the ability to analyze complex information based on the Review Protocol and/or the guidance from the lead supervising attorney.
- Strong oral and written communication skills as well as excellent listening skills.
- Ability to follow instructions and, when necessary, ask clear and concise questions.
- Basic understanding of how technology is applied to manage the collection, retrieval, processing, analysis, and production of documents.
- Efficient, Dependable, Conscientious, and Flexible Candidates based out of smaller cities and emerging review markets.

1L Review - Licensed document reviewers.

Privilege Review - Licensed document reviewers hand-selected and approved by client for higher-value work.

Team Lead / QC - Senior level licensed document reviewers responsible for quality assurance and first-line team oversight.

Associate Review Manager - Senior level licensed document reviewer with significant experience managing the quality control process, generally works under a Review Manager and assists the Review Manager with reporting and Client communications.

Review Manager - Direct oversight of review team by licensed attorney manager with significant understanding of legal process and requirements for running successful document review project.

Pricing Special Services

Tape Services	Unit	USD	Notes
Tape Catalog	Tape	35.00	Generate File Listing Reports from Tapes.
Tape Restore	Tape	250.00	Includes restoration of data from tape source from standard unencrypted tapes and backup software.
Complex Tape Handling	Tape	100.00	Restoring data from non-standard tape source or backup software (in addition to the Tape Restore fee).
Encrypted Tape Handling	Tape	300.00	Support for Commvault & BackupExec (software based encryption). Encryption key must be provided (in addition to the Tape Restore fee).
Custodian Level Extraction	Custodian	150.00	Identify and extract data for specified custodians (in addition to the Tape Restore fee).
Data Deduplication	Tape	200.00	De-Duplicate all file level data for native delivery (in addition to the Tape Restore fee).
	GB	35.00	
	Tape	750.00	

Data Email Deduplication	GB	35.00	De-Duplicate all file level and email data for native delivery (in addition to the Tape Restore fee).
PST Extraction	EDB	150.00	Extract mailbox from Exchange Database (EDB) to be delivered in PST format (Additional fee applicable for De-duplication of data) and in addition to the Tape Restore fee.
Data Recovery	Unit	USD	Notes
Data Recovery	Hour	250.00	Recover data from USB, Laptop, Desktop, SSD storage media.
Data Recovery from Servers - Evaluation	Hour	250.00	Evaluation to check feasibility of recovery and rebuild data from Failed RAID servers. This would also include Virtual Machines. Total cost for recovery will be determined after evaluation.
Data Recovery from Phones	Device	650.00	Attempt to bypass damage phone.
Hard Copy	Unit	USD	Notes
	Page Low	0.09	

Scanning Services	Page High	0.20	B&W Hard Copy Scanning. Price based on grade or quality of documents to be scanned, to be determined after review of documents.
Oversized Scanning	Square Foot	1.25	Scanning of oversized documents.
OCR	Page	0.02	OCR of Scanned Images.
Blowbacks	Page	0.06	Provide hardcopy of Tiff or PDF images.
Logical Document Determination (LDD)	Image	0.04	Document unitization. Logically determine document breaks
Coding	Field Doc	0.06	Bibliographic - Objective fields
Nebula Archive	Intelligent	Unit	USD
			Notes
			Enterprise-grade archiving solution.
Nebula Intelligent Archive – Migration Fee	TB	Available Upon Request	Acquire data from client data sources and ingest into Nebula Intelligent Archive.
Nebula Intelligent Archive – Nebula Data Transfer	GB	Available Upon Request	Transfer data from Nebula Intelligent Archive to Nebula Import module.

Nebula Intelligent Archive – Enhanced Archive Storage	TB Month	Available Upon Request	Monthly hosting fee for data stored in Nebula Intelligent Archive. Includes full-text index for all data, retention and disposition policies, and disaster recovery backup.
Nebula Intelligent Archive – Export	GB	Available Upon Request	Fee to export data from Nebula Intelligent Archive.
Nebula Intelligent Archive – Technical Solutions	Hour	Available Upon Request	Billable operations or custom development time. Technical support for Nebula Intelligent Archive. Support time is rounded up to 30-minute increments. After hours, weekends & holidays billed at standard rate.
Nebula Intelligent Archive – Professional Services	Hour	Available Upon Request	Consulting Services including but not limited to information governance, legal hold inventory preparation and validation, legal hold implementation and management in Nebula Intelligent Archive.
Legal Hold	Unit	USD	Notes
Legal Hold		Available Upon Request	Please contact our Compliance, Information Governance, and Archiving Team for consult.

8. Additional Pricing Terms

The Contractor is encouraged to offer quick payment terms. The number of days must not include processing time for payment to be received by the Contractor's financial institution.

Quick payment terms: 3 % discount off invoice if paid within 15 days after receipt of invoice.

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

Travel and Expenses

The State does not pay for overtime or travel expenses.

SCHEDULE C - INSURANCE REQUIREMENTS

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

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

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

7. **Limits of Coverage & Specific Endorsements.**

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Personal & Advertising Injury \$2,000,000 Products/Completed Operations \$2,000,000 General Aggregate	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
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:	Contractor must have their policy cover information security and privacy liability, privacy

Required Limits	Additional Requirements
\$1,000,000 Each Occurrence \$1,000,000 Annual Aggregate	notification costs, regulatory defense and penalties, and website media content liability.
Professional Liability (Errors and Omissions) Insurance	
Minimum Limits: \$3,000,000 Each Occurrence \$3,000,000 Annual Aggregate	

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

SCHEDULE D – SERVICE LEVEL AGREEMENT

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 Terms and Conditions.

“**Actual Uptime**” means the total minutes in the Service Period that the Hosted Services are Available.

“**Availability**” has the meaning set forth in **Section 1.1**.

“**Availability Requirement**” has the meaning set forth in **Section 1.1**.

“**Available**” has the meaning set forth in **Section 1.1**.

“**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 **Section 2.9**.

“**Critical Service Error**” has the meaning set forth in **Section 2.5**.

“**Exceptions**” has the meaning set forth in **Section 1.2**.

“**High Service Error**” has the meaning set forth in **Section 2.5**.

“**Low Service Error**” has the meaning set forth in **Section 2.5**.

“**Medium Service Error**” has the meaning set forth in **Section 2.5**.

“**Resolve**” has the meaning set forth in **Section 2.6**.

“**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 **Section 1.3**.

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

“**Service Availability Credits**” has the meaning set forth in **Section 1.6(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 **Section 2.8**.

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

“**Service Period**” has the meaning set forth in **Section 1.1**.

“**Software Support Services**” has the meaning set forth in **Section 2**.

“**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 phone support 8 am to 5 pm ET Monday – Friday excluding State Holidays.

“**Support Request**” has the meaning set forth in **Section 2.5**.

“**Support Service Level Requirements**” has the meaning set forth in **Section 2.4**.

1. Service Availability and Service Available Credits.

1.1 Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a “**Service Period**”), at least 99.98% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the “**Availability Requirement**”). “**Available**” means the Hosted Services and Software are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract. “**Availability**” has a correlative meaning. The Hosted Services and Software are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services and Software, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: $(\text{Actual Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \div (\text{Scheduled Uptime} - \text{Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception}) \times 100 = \text{Availability}$.

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

- (a) Failures of the State’s or its Authorized Users’ internet connectivity;

(b) Scheduled Downtime as set forth in **Section 1.3**.

1.3 Scheduled Downtime. Contractor must notify the State at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services or Software in whole or in part (“**Scheduled Downtime**”). All such scheduled outages will: (a) last no longer than eight (8) hours; (b) be scheduled between the hours of 10:00 p.m. and 6:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

1.4 Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

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

1.6 Remedies for Service Availability Failures.

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

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

<95.0%	100%
--------	------

(b) Any Service Availability Credits due under this **Section 1.6** will be applied in accordance with payment terms of the Contract.

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

2. Support and Maintenance Services. Contractor will provide IT Environment Service and Software maintenance and support services (collectively, “**Software Support Services**”) in accordance with the provisions of this **Section 2**. 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.

2.1 Support Service Responsibilities. Contractor will:

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

(b) provide unlimited telephone support 8 am to 6 pm ET Monday - Friday excluding State Holidays.

(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 2**.

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

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

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

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

- (i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;
- (ii) If Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 2.5 and 2.6**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and
- (iii) Notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

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

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

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

2.4 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 2.4 ("Support Service Level Requirements")**, and the Contract.

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

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	<ul style="list-style-type: none"> • Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions.
High Service Error	<ul style="list-style-type: none"> • Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	<ul style="list-style-type: none"> • IT Environment Services and Software is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work around.
Low Service Error	<ul style="list-style-type: none"> • Request for assistance, information, or services that are routine in nature.

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

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	One (1) hour	Three (3) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
High Service Error	One (1) hour	Four (4) hours	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour or portion thereof that the	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-

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)
			corresponding Service Error is not responded to within the required response time.	Resolved, which amount will thereafter double for each additional one-hour increment.
Medium Service Error	Three (3) hours	Two (2) Business Days	N/A	N/A
Low Service Error	Three (3) hours	Five (5) Business Days	N/A	N/A

2.7 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.

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

2.9 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.

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

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

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

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

3.4 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 2 hours, and a Recovery Time Objective (RTO) of 4 hours (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the

Hosted Services. Contractor’s current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule F**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 3**; and provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor’s receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

4. Professional Services. Contractor represents and warrants that its professional services shall be performed by competent personnel and shall be of professional quality consistent with generally accepted industry standards for the performance of such services and shall comply in all respects with the requirements of this Contract and the specifications set forth in the Statement of Work. The following table represents examples of breaches of the foregoing warranty, which will entitle the State to the corresponding credit set forth below:

Warranty Breach	Credit of Fees
Missed Production Deadline	50% credit for all Fees related to the affected matter for the month in which the deadline was missed.
Overbilling or Invoicing Errors (e.g. billing license fees to the wrong matter)	For each billing mistake on an invoice to which the total fees are overbilled by more than 5%, the State shall receive a 10% credit for all Fees related to the affected matter for the month that corresponds with the invoice. For example, if an October 2024 invoice contains three billing mistakes, there would be a 30% credit for all October 2024 Fees related to the affected matter). Credits under this provision are capped at 100% of all Fees related to the affected matter for the month that corresponds with the invoice. (For example, if an October 2024 invoice contains 12 billing mistakes, the credits under this provision would be capped at 100% of the October 2024 Fees related to the affected matter).

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

Level	CONTACT
1	Jay Horowitz SVP Global Solutions Strategy jay.horowitz@kldiscovery.com 917-751-9796 Pat Colon Director, Strategic Integrations pat.colon@kldiscovery.com Tel: 646-949-2158
2	Ashley Cammack Director US LT Project Management ashley.cammack@kldiscovery.com -571-585-0332
3	Meghan DelMonaco VP Global LT Project Management meghan.delmonaco@kldiscovery.com 703-727-5481
4	Ferdinand Cami VP Global Hosted Services Ferdinand.cami@kldiscovery.com +1-733-865-2907
5	Danny Zambito Chief Operating Officer Danny.zambito@kldiscovery.com 1-703-349-9603

SCHEDULE E – DATA SECURITY REQUIREMENTS

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

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

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

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

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

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

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

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

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

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

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

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

(a) ensure the security and confidentiality of the State Data;

(b) protect against any anticipated threats or hazards to the security or integrity of the State Data;

- (c) protect against unauthorized disclosure, access to, or use of the State Data;
- (d) ensure the proper disposal of any State Data in Contractor's or its subcontractor's possession; and
- (e) ensure that all Contractor Representatives comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html.

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

4. Acceptable Use Policy. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.

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

5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause pursuant to **Section 15.1** of the Contract;

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit based on State

required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs.

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

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 the requirements of the State's data security policies as set forth in this Contract, and must, at a minimum, remain compliant with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

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

5.6 take all reasonable measures to:

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

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

5.7 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;

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

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

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

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

8. Security Audits.

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

8.2 Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the

commencement of Services and from time to time during the term of this Contract. The State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. If the State chooses to perform an on-site audit, Contractor will, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least ten (10) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Hosted Services and their housing facilities and operating environments.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10. Infrastructure Scanning.

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

11. Nonexclusive Remedy for Security Breach.

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

Schedule E, Attachment 1

SAFEGUARD REQUIREMENTS OF CONFIDENTIAL TAX DATA

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

I. Authority

Authority for the Michigan Department of Treasury to require that this section be included in the Contract is contained in 1941 PA 122, as amended, MCL 205.28(1)(f), which subjects current or former contractors to the same restrictions and penalties imposed upon department employees regarding the treatment of confidential information. A private contractor or its employees are strictly prohibited from disclosing taxpayer information to a third party. The prohibition against disclosure does not bar an employee of a private contractor with whom the State of Michigan (State) contracts that processes tax returns or payments pursuant to the Contract from having access to confidential information that is reasonably required for the processing or collection of amounts due this State. Private contractors and any subcontractors will follow Treasury guidelines for Authorized representatives.

II. Confidentiality

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

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

Confidential information obtained under this contract will not be disclosed except as required by state law, or in the proper administration of applicable laws, promulgated rules and procedures. In the event, confidentiality statutes are amended, Treasury will notify Contractor of any changes. No employee, agent, authorized representative or legal representative of Contractor will disclose any information obtained by virtue of this section to any other division within their company or any other governmental agency, department or unit within such governmental agency whether local, state, federal or foreign, department or unit within such governmental agency, or any unauthorized third party. No tax returns or tax return information accessed by Contractor will be duplicated or disseminated within or outside the company without the written approval of the Contract Compliance Inspector. Tax returns and tax return information remain the property of Treasury.

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

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

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

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

MCL 205.27(4) states:

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

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

III. Procedure for Security

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

- A. Access to the tax returns and tax return information will be allowed only to those authorized employees and officials of Contractor who need the information to perform their official duties in connection with the uses of the information authorized in this Contract.
- B. Any records created from tax returns and tax return information will be stored in an area that is physically safe from access by unauthorized persons during duty hours and locked in a secure area during non-duty hours, or when not in use.
- C. Any records matched and any records created by the match will be processed under the immediate supervision and control of authorized personnel in a manner in which will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve any such records by means of a computer, remote terminal or other means.
- D. All personnel who will have access to the tax returns and tax return information and to any records created by the tax return information will be advised annually of the confidential nature of the information, the safeguards required to protect the information and the civil and criminal sanctions

for noncompliance contained in MCL 205.28 (2) and MCL 205.27(4) and will sign confidentiality certifications.

- E. All confidential information, electronic and paper, will be secured from unauthorized access and with access limited to designated personnel only. State tax return information will not be commingled with other information. All Michigan tax returns and return information will be marked as follows: **CONFIDENTIAL - DO NOT DISCLOSE - MICHIGAN TREASURY TAX RETURN INFORMATION**
- F. Treasury, Office of Privacy and Security or Contract Compliance Inspector may make onsite inspections or make other provisions to ensure that adequate safeguards are being maintained by the Contractor.
- G. The Treasury Office of Privacy and Security may monitor compliance of systems security requirements during the lifetime of the Contract or any extension.
- H. Contractor will also adopt policies and procedures to ensure that information contained in their respective records and obtained from Treasury and taxpayers will be used solely as stipulated in the Contract.

IV. Computer System Security of Tax Data

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

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

A. Controlled Access Protection

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

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

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

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

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

b) Operating Features of System Security

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

- i. Access rights to confidential tax information must be secured through appropriate levels of authorization.
- ii. An audit trail must be maintained of accesses made to confidential information.
- iii. All confidential and protected information must be cleared from a system before it is used for other purposes not related to the enforcement, collection or exchange of data not covered by this section or by an addendum to this Contract.
- iv. Hard copies made of confidential tax return information must be labeled as confidential information.
- v. Confidential Treasury tax information will be blocked or coded as confidential on system.
- vi. Any computer system in which Michigan tax return information resides must systematically notify all users upon log-in of the following disclosure penalties for improperly accessing or making an authorized disclosure of Michigan tax return information:

NOTICE TO EMPLOYEES AND AUTHORIZED REPRESENTATIVES

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

MICHIGAN PENALTIES

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

- Criminal penalties up to \$5,000 and/or imprisonment for 5 years, plus costs and dismissal from employment if it is found that a current or former employee or authorized representative has made an unauthorized disclosure of a tax return or tax return information or divulged audit selection or processing parameters. [MCL 205.28(2)]
- A misdemeanor, punishable by a fine of not more than \$1,000.00, or imprisonment for not more than 1 year, or both if the person is not in violation pursuant to MCL 205.27(2), but who knowingly violates any other provision of this act, or of any statute administered under this act.

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

- 3) **Assurance** – Contractor must ensure that all access controls and other security features are implemented and are working when installed on their computer system. Significant enhancements or other changes to a security system must follow the process of review, independent testing, and installation assurance. The security system must be tested at least annually to assure it is functioning correctly. All anomalies must be corrected immediately.
 - a) The Contractor must initiate corrective action for all non-conformities as soon as detected and immediately advise the Contract Compliance Inspector. Notice of the corrective action must be provided to the Contract Compliance Inspector. All non-conformities must be reported to the Contract Compliance Inspector with the following:
 - a. Duration of non-conformity/interruption
 - b. Reason for non-conformity/interruption
 - c. Resolution.
 - b) All non-conformities to the specifications/tasks of the Contract must be corrected within four (4) hours. The State recognizes there will be instances when adherence to this time frame will not be possible. However, the State will only tolerate this on an exception basis. To request an exception to this time frame, the Contractor must submit a detailed project plan to address the non-conformity within four (4) hours to the Contract Compliance Inspector for approval.
- 4) **Documentation** – Design and test documentation must be readily available to the state. The developer or manufacturer should initially explain the security mechanisms, how they are implemented and their adequacy (limitations). This information should be passed on to the security officer or supervisor. Test documentation should describe how and what mechanisms were tested and the results. If recognized organizations/tests/standards are used, then a document to that effect will suffice. For example, a system that has been tested and

certified as meeting certain criteria may have a document stating this fact, without detailed tests/results of information. Contractor, however, must ensure the documentation covers the exact system and that it includes the specific computer system used by Contractor.

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

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

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

V. Electronic Transmission of Michigan Tax Information

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

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

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

A. Remote Access

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

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

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

B. Portable Computer Devices

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

VI. Record Keeping Requirements for Information Received

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

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

The Contractor will adopt and implement formal procedures to:

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

A. Electronic Media

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

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

B. Recordkeeping Requirements of Disclosure Made to State Auditors

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

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

VII. Contract Services

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

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

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

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

- B. An acknowledgment that a taxpayer has filed a return is known as a "fact of filing" and may not be disclosed. All tax return data made available in any format will be used only for the purpose of carrying out the provisions of the Contract between Contractor and the sub-contractor.

Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract between Contractor and the subcontractor. In addition, all related output will be given the same level of protection as required for the source material.

- C. The subcontractor will certify that the data processed during the performance of the Contract between Contractor and the subcontractor will be completely purged from all data storage components of the subcontractor's computer facility, and no output will be retained by the subcontractor at the time the work is completed.
- D. Destruction of tax data, including any spoilage or any intermediate hard copy printout which may result during the processing of Michigan tax return information, will be documented with a statement containing the date of destruction, description of material destroyed, and the method used. Destruction parameters must meet the standards of Section IX, Disposal of Tax Information, of this agreement.
- E. Computer system security and physical security of tax data stored and processed by the subcontractor must be in compliance with security guidelines and standards established by this contract. See section VI (Record Keeping Requirements for Information Received in Paper Format) for more details.
- F. The Contractor will be responsible for maintaining a list of employees authorized to access Michigan tax return information and will provide a copy of such list to Treasury.
- G. No work involving information furnished under the contract will be subcontracted without the specific approval of Treasury. Contractor and approved subcontractors handling Michigan tax return information will be required to sign the *Vendor, Contractor or Subcontractor Confidentiality Agreement* provided by Treasury, (Form 3337, see Attachment A). The original agreements will be returned to the Disclosure Officer for the Department of Treasury and a copy sent to the Contract Compliance Inspector.

VIII. Transport of Tax Information

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

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

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

IX. Disposal of Tax Information

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

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

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

X. Security Responsibility

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

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

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

XI. Security Breach Notification

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

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

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

XII. Certification of Compliance

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

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

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

XIII. Effective Date

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

Attachment A

Reset Form

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

Vendor, Contractor or Subcontractor Confidentiality Agreement

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

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

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

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

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

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

Michigan Penalties

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

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

City Penalties

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

Federal Penalties

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

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

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

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

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

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

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

Reset Form

Incident Report

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

PART 1: A. CONTACT INFORMATION (Reporting Entity)			
Full Name (Last, First, Middle Initial)		Division/Office	
Telephone Number	Fax Number	E-Mail Address	
B. CONTACT INFORMATION (Affected Entity)			
Full Name (Last, First, Middle Initial)		Division/Office	
Telephone Number	Fax Number	E-Mail Address	
PART 2: INCIDENT INFORMATION			
Whose information was involved in the incident? <input type="checkbox"/> Treasury <input type="checkbox"/> Federal Tax Information <input type="checkbox"/> Other State Agency, specify _____ <input type="checkbox"/> Other _____			
Incident Category (select all that apply)			
<input type="checkbox"/> Passwords Shared/Stolen	<input type="checkbox"/> Computer Virus/Spam	<input type="checkbox"/> Paper Archives Compromised	
<input type="checkbox"/> Misrouted Communications	<input type="checkbox"/> Data Destruction/Deletion	<input type="checkbox"/> Safe/Lockbox/other Compromise	
<input type="checkbox"/> Unauthorized Access	<input type="checkbox"/> Backups Missing or Stolen	<input type="checkbox"/> Delivery of Documents Lost	
<input type="checkbox"/> Fraudulent Actions	<input type="checkbox"/> Hacking of Networks/Systems	<input type="checkbox"/> Inappropriate Destruction Paper	
<input type="checkbox"/> Lost/Stolen Information/Data	<input type="checkbox"/> Improperly Secured Sys/Web	<input type="checkbox"/> Inappropriate Destruction Media	
<input type="checkbox"/> Lost/Stolen Cash/Checks	<input type="checkbox"/> Circumvention of Security Protocols	<input type="checkbox"/> Lost/Stolen Equipment	
<input type="checkbox"/> Inappropriate Building Access	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
Incident Affects			
<input type="checkbox"/> Financial Information/Resources	<input type="checkbox"/> Personal Information (SSN, Driver License No, Financial information)	<input type="checkbox"/> Unauthorized/Unlawful Activity	
<input type="checkbox"/> Confidential/Sensitive Information	<input type="checkbox"/> Human Resources (threat)	<input type="checkbox"/> Other _____	
Date Incident Occurred	Time Incident Occurred	Date Incident Discovered	Time Incident Discovered
Incident Location		Number of Individuals Affected	
Involved Parties/Entities		Does this involve personal information (first and last name along with a SSN, driver license number, or credit/debit card account number)? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Date of Initial Report			
Description of Incident			

PART 1: CONTACT INFORMATION (Affected Entity)			
Full Name (Last, First, Middle Initial)		Division/Office	
PART 3: INCIDENT RESOLUTION			
Notification issued to affected individuals? <input type="checkbox"/> Yes <input type="checkbox"/> No	How many notifications were sent?	Breach Notification Method? <input type="checkbox"/> E-mail <input type="checkbox"/> Telephone <input type="checkbox"/> US Mail <input type="checkbox"/> Web	
Who was notified?		Date notification was issued	
Incident Cost <input type="checkbox"/> Check if incident costs are less than \$250. If \$250 or more, complete the detailed summary of costs below.			
<u>Manhours:</u>		<u>Other:</u>	
Treasury \$ _____		Postage \$ _____	
DTMB-OES \$ _____		Credit Monitoring Service \$ _____	
DTMB-Treasury Agency Services \$ _____		_____ \$ _____	
		Total Cost of Incident \$ _____	
Action Taken			
Incident Impact			
Post Incident Recommendations			
PART 4: REPORT PREPARER INFORMATION			
Final Report Prepared By:	Date Prepared	Preparer Title	Preparer's Telephone Number
Preparer Signature			Date
OFFICE OF PRIVACY AND SECURITY USE ONLY			
Administrator, Office of Privacy and Security Signature			Date

Schedule E – Attachment 2
Exhibit 7 IRS Publication 1075

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

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

- (1) All work will be performed under the supervision of the contractor.
- (2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- (7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- (8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- (9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- (10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities

which the contractor assumes toward the agency under this contract.

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

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

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

II. CRIMINAL/CIVIL SANCTIONS

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

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

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

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

(5) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 ([see Exhibit 4, Sanctions for](#)

Unauthorized Disclosure, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

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

Schedule E – Attachment 3

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

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

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

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

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

1.00 Definitions

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

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

2.00 Responsibilities of the Contracting Government Agency.

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

3.00 Responsibilities of the Contractor.

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

4.00 Security Violations.

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

- 4.02 Security violations can justify termination of the appended agreement.
- 4.03 Upon notification, the FBI reserves the right to:
- a. Investigate or decline to investigate any report of unauthorized use;
 - b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.
- 5.00 Audit
- 5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.
- 6.00 Scope and Authority
- 6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.
- 6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.
- 6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
- 6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.
- 6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

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

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

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

SCHEDULE G – Transition in and Out

Contractor's team provided during the transition period will be the same as the team that will be working with the State going forward (Account Executive, PM Director, PM Leads, Deputies, Assistant PMs, etc.). Contractor's team will work with State to develop a detailed transition plan, with stated objectives over a transition period. During the transition period, specific action items will of course require the input of other Contractor stakeholders, ranging from IT security, data processing and billing specialists, who will be brought in as needed to handle specific transition-related tasks. To enhance and improve the State's processes, Contractor may need specialized input from Contractor's Advisory team or eDiscovery technologists (i.e., with respect to tweaking the State's existing priv screen).

The Account Executive, PM Director and Review Director coordinate the involvement of specific individuals or groups. Multiple tracks will be moving simultaneously during transition. There may be meetings about billing requirements, setting Contractor up for e-billing, etc. that occur on the same day that there may be 2-3 meetings involving the State for specific matter set up and processing directions.

Communication will be key throughout the transition to eliminate and or mitigate risk during the transition planning. Starting a new relationship should be viewed as an opportunity to strengthen and "clean-up" the State's existing protocols. It is an opportunity to keep what is working and eliminate what is not. It is an opportunity to introduce better ways to do the needed tasks. The State's existing processes around the launch process can be analyzed and discussed; past challenges to this process can be addressed, and the processes can be optimized through minor (or major) tweaks and modifications.

The draft implementation plan timeline includes a basic timeline and introduces resource groups that will be needed. These will be customized (tailored) based on the exact needs of the State. In summary, presuming a timeline where the State's eDiscovery team is amenable to substantially focusing on project startup and transitions with Contractor's team, a one-to-two- week startup/transition period is anticipated. The time frames and frequency for these tasks will be adjusted according to the State's preferences and project/portfolio needs.

After the kick-off meeting is held with the State, Contractor will detail the specific deliverables and timeline for delivery for the State's specific needs.

Implementation will begin with the signing of the contract. Contractor's Client Services team along with members of Contractor's Project Management team will schedule a meeting to discuss the State of Michigan Playbook. This meeting will determine a timeline for working with the State to complete the various items including the project kick-off checklist, database specifications, processing specifications, production specifications, custom reporting requests and billing requirements, and will begin

discussions on the State's preferred workflows for use across matters. Ideally, these Playbook sessions will occur over the course of the first 2 weeks to have solid documentation to use for setting up the State's environment appropriately and begin training sessions with the State's team members. New projects can begin during this phase. The Playbook development requires dedicated time from both the State and Contractor to be successful.

If the State chooses to migrate data into Contractor's environment, Contractor has workflows already in place to ease that transition. Upon review of the data with the State team, Contractor's data migration team will develop a custom migration plan based on the details such as number of databases, data volume, and status of each matter to best minimize the impact on the State's case teams. The schedule for data migration will vary based on factors such as data volume, case activity, and if Contractor is able to work on the migration 24/7 or will be limited to nights and/or weekends.

Once the implementation is underway, development of the training agenda can begin.

Based on the desires of the State, Contractor will draft training agendas for New Users, Power Users, and Administrators. These training agendas will include items such as the basic knowledge to be provided at each level along with the State's-specific workflows, technology integrations, and policies. Training will be performed via MS Teams. The training agendas drafted will become part of the State of Michigan Playbook and be used on all matters unless otherwise specified. By having this training criteria in place for all matters, the State can be sure that the State's user's are utilizing the technology components to their best ability to streamline the review and create cost efficiencies.

Training sessions are typically one hour and cover the specifics needed for that group of attendees. Contractor can design longer sessions that allow attendees to leave the call, after the information specific to their role is covered. Contractor can also schedule multiple sessions targeting the needs of each team

The training agenda would be as follows:

1. Basic overview of Nebula and its overall functionality. Basic overview of all proprietary applications in Nebula.
2. Comprehensive instruction on how to ingest data into Nebula and utilize the Culling module.
3. Comprehensive instruction on how to best utilize the ECA functionality within Nebula.
4. Comprehensive training on how to work in the Review module of Nebula, to include various admin functions, such as updates to coding layouts and choices, how to adjust document views, redaction options (including the AutoRedaction, Native Spreadsheet Redaction, and Audio/Visual Redaction apps), mass actions including mass tagging, search options, and how to adjust permissions.
5. Comprehensive training on the applications to understand how they are used

and how they could be added to the State of Michigan's workflows and processes for each matter. The applications include, AutoRedaction, A/V Suite, Multi-Matter Management, Native Spreadsheet Redaction, and Automated Workflow. This can also include the use of the Predictive Coding application.

6. Comprehensive training on the use of analytics to include each feature of Contractor's Analytics. This training would cover structured analytics first (email threading, near dupe ID, language detection) and then Predictive Coding/TAR projects. Training on how to utilize analytics during production quality control to further limit the risk of inadvertent production of privileged or confidential documents is recommended.
7. Comprehensive training on how to complete and export productions from Nebula to include quality control protocols.

As well as having access to in-person and remote training sessions with experienced trainers, users will have access to a range of e-learning and self-service resources, at all times. These include:

- The online Nebula help guide which provides full explanatory information on all Nebula features along with clear, easy-to-follow step-by-step instructions for performing many tasks in Nebula.
- Nebula Academy for video-based self-paced learning and application certification through Reviewer Fundamentals to Advanced Nebula Reviewer skills.

The State of Michigan Hosted ECA Platform Delivery Team

A support team shall be required to support the production system for issue resolution, new user onboarding, functionality enhancement requests, bug fixes, disaster recovery exercises, and help desk support. Other support activities shall encompass report building, service level agreement metrics, production troubleshooting, and platform maintenance notifications. This team is organized as shown below.

Roles and Responsibilities

Relationship Manager (Jay Horowitz, SVP Global Solutions Strategy)

– Responsible for overall relationship, negotiating and agreeing to business terms, strategic development, and executive sponsorship.

Delivery Manager (Danny Zambito, SVP, Global Legal Technologies) –

Responsible for overall delivery, user support, system performance, and executive sponsorship.

Implementation Manager (Eric Robinson, Managing Director Global Advisory Services & Strategic Client Solutions) –

Responsible for development and execution of implementation plan as well as day-forward operations.

Portfolio Manager (Ashley Cammack, Director, US LT Project Management) –

Responsible invoicing, reporting, and all administrative/business operation

deliverables.

Information Security Manager (Jason Davison, VP, Information Security) – Responsible for implementation and execution of information security plan.

Nebula Support Manager (Ferdinand Cami, VP, Hosted Solutions) – Responsible for application performance and end user service delivery.

R&D Manager (Anthony DeJohn, VP, Advanced Technologies) – Responsible for application development, engineering, and roadmap planning and execution.

Infrastructure Manager (Dustin Allen, VP, Information Technology) – Responsible for delivery, operation, and maintenance of the Hosted ECA environment.

Application Support Manager, (Lee Colvin, Director, Application Support) – Responsible for overall application performance.

User Support Manager, (Greg Schmitz, Director, End User Support) – Responsible for end-user service delivery.

Sample Implementation Timeline

Task Name	Duration	Predecessors	Resources
Master Services Agreement	2 wks		Contractor's Contract Team; The State's Legal Team
Finalize State of Michigan's Dedicated Project Management Team	2 days	MSA	Contractor's Project Team
On-Site Review of State of Michigan Systems to Migrate (if needed)	2 days	MSA	Contractor's Data Migration Team; The State's Team
On-Site Playbook Kick-off	2 days	MSA	Contractor's Managed Services Team; The State's eDiscovery Team

Development of The State of Michigan Playbook	2 wks	MSA	Contractor's Managed Services Team; The State's eDiscovery Team
Finalize Draft of Migration Plan	1 wk	MSA	Contractor's Data Migration Team; The State's IT/eDiscovery Team
Data Migration and QC Phase	TBD	MSA/Migration Plan	Contractor's Data Migration Team; The State's IT/eDiscovery Team
Administrator Training	8 hours	MSA/Playbook	Contractor's Training Team; The State's eDiscovery Team
Implementation Pre-Meeting	3 hours	MSA/Playbook	Contractor's Delivery Team; The State's eDiscovery Team
Implementation Meetings	TBD	MSA/Playbook	Contractor's Delivery Team; Contractor's Project Mgmt; The State's eDiscovery Team
End User (Reviewer) Training Sessions	2 wks	MSA/Playbook/Implementation	Contractor's Training Team; The State's eDiscovery Team

Schedule H HIPAA BUSINESS ASSOCIATE AGREEMENT

The parties to this Business Associate Agreement (“Agreement”) are the Michigan Department of Technology, Management & Budget (“DTMB”, “Business Associate 1”) on behalf of **Michigan Department of Attorney Generals** (“Covered Entity”) and **KLDiscovery Ontrack LLC d/b/a KLDiscovery** “Business Associate 2”.

RECITALS

- A. Under this Agreement, Business Associate 2 will collect or receive certain information on the Covered Entity’s behalf, some of which may constitute Protected Health Information (“PHI”). In consideration of the receipt of PHI, the Business Associate agrees to protect the privacy and security of the information as set forth in this Agreement.
- B. Covered Entity and each Business Associate intend to protect the privacy and provide for the security of PHI collected or received by the Business Associate under the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and the HIPAA Rules, as amended.
- C. The HIPAA Rules require the Covered Entity to enter into an agreement containing specific requirements with Business Associate 1, and likewise Business Associate 1 must enter an agreement with Business Associate 2 before the Business Associate 2’s receipt of PHI.

AGREEMENT

1. Definitions.

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

b. “Business Associate” has the same meaning as the term “business associate” at 45 CFR 160.103 and regarding this Agreement means DTMB (“Business Associate 1”) and **KLDiscovery Ontrack LLC d/b/a KLDiscovery** (“Business Associate 2”).

c. “Covered Entity” has the same meaning as the term “covered entity” at 45 CFR 160.103 and regarding this Agreement means the **Michigan Department of Health and Human Services (“MDHHS”), Michigan Department of Veteran and Military Affairs (“MDVMA”) and/or Michigan Office of Retirement Services (“MORS”)**.

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

2. Obligations of Business Associate 2.

Business Associate 2 agrees to:

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

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

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

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

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

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

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

PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure. If the request for an accounting is delivered directly to Business Associate 2 or its agents or subcontractors, Business Associate 2 must, within ten days of the receipt of the request, forward it to the Covered Entity in writing.

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

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

j. retain all PHI throughout the term of the Agreement and for a period of six years from the date of creation or the date when it last was in effect, whichever is later, or as required by law unless deletion of PHI is requested in writing, or the matter has ended in which case Business Associate 2 shall delete all data if requested by Covered Entity. This obligation survives the termination of the Agreement.

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

l. within thirty days of a written request by the Covered Entity, not to exceed once per calendar year, except for good cause shown, subject to reasonable confidentiality undertakings being given Business Associate 2 and its agents or subcontractors must allow the Covered Entity to conduct a reasonable inspection of the facilities while accompanied, documentation concerning the systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI under this Agreement. Business Associate 2 and the Covered Entity will mutually agree in advance upon the scope, timing and location of such an inspection. Covered Entity must protect the confidentiality of all confidential and proprietary information of Business Associate 2 to which the Covered Entity has access during the course of such inspection. Covered Entity and Business Associate 2 will execute

a nondisclosure agreement, if requested by the other party. The fact that the Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate 2's facilities, documentation concerning systems, books, records, agreements, policies and procedures does not relieve Business Associate 2 of its responsibility to comply with this Agreement. Covered Entity's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, does not constitute acceptance of such practice or a waiver of the Covered Entity's enforcement rights under this Agreement.

3. Permitted Uses and Disclosures by the Business Associate.

a. Business Associate 2 may use or disclose PHI:

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

(2) as required by law;

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

(4) to de-identify, consistent with 45 CFR 164.514(a) – (c), PHI it receives from the Covered Entity. If Business Associates 2 de-identifies the PHI it receives from the Covered Entity, Business Associate 2 may use the de-identified information for any purpose not prohibited by the HIPAA Rules; and

(5) for any other purpose listed here: **[describe how Business Associate 2 will use and/or disclose PHI under this Agreement].**

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

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

4. Covered Entity's Obligations

Covered entity agrees to:

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

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

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

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

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

6. Termination.

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

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

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

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

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

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

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

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

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

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

(5) return to the Covered Entity (or, if agreed to by the Covered Entity in writing, destroy) the PHI retained by Business Associate 2 when it is no

longer needed by Business Associate 2 for its proper management and administration or to carry out its legal responsibilities.

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

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

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

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

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

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

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

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

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

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

17. Representatives and Notice.

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

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

Covered Entity Michigan Department of Health and Human Services Representative:

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

Covered Entity Michigan Department of Military and Veteran Affairs Representative:

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

Covered Entity Michigan Office of Retirement Services Representative:

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

Business Associate 1 Representative:

Name: Dustin Senneker
Title: Assistant Attorney General
Department: Attorney Generals
Address: 525 W Ottawa St, Lansing, MI 48933
Phone: 517-335-7573
Email: sennekerd@michigan.gov

Business Associate 2 Representative:

Name:
Title:
Department:
Address:

Phone:
Email:

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

**AG as Business Associate 1, on
behalf of MDDHS,MDMVA, and
MORS**

Business Associate 2

[INSERT NAME]

By: _____

By: _____

Date:

Date: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____