STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget

320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **MA240000000752**

CONTRACTOR	Metrc LLC
	4151 S. Pipkin Road
	Lakeland FL 33811
	JUSTIN GREEN
	772-633-3240
	JUSTIN.GREEN@METRC.COM
	VS0039548

STATE	Program Manager	Various	Various
	Contract Administrator	Jarrod Barron	DTMB
		5172490406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY

Cannabis Rules Monitoring System

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
	May 7, 2029	5 - 12 Months	June 7, 2029

PAYMENT TERMS	DELIVERY TIMEFRAME
Net 45	N/A

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
□ P-Card □ Direct Voucher (PRC) □ Other	☒ Yes □ No

MINIMUM DELIVERY REQUIREMENTS

N/A

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
□		□		

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$1,923,000.00	$2,000,000.00	$3,923,000.00

DESCRIPTION

Effective 10/1/2024, the parties increase the annual payment to Metrc by $2 million for the term of the contract for the CRA to pay User Fees that are currently billed to CRA licensees. Beginning 10/1/2025, this annual payment will be adjusted each year by the 12-month Consumer Price Index rate set the preceding December 31 using the US Bureau of Labor Statistics "All items less food and energy" category and amended to the contract via an annual Contract Change Notice. All unpaid balances of CRA Licenses prior to 10/1/2024 remain fully due, and the CRA licensees will remain obligated to pay those. All other terms, conditions, specifications, and pricing remain the same. Per Contractor, Agency, DTMB Procurement and State Administrative Board approval on 9/10/2024. Available Ad Board funds after this change notice is $249,999.99.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
LARA	Cole Thelen	517-388-8350	ThelenC10@michigan.gov
DTMB	Stuart Willard	517-526-5410	WillardS@michigan.gov

STATE OF MICHIGAN
PROCUREMENT
Michigan.gov/MiProcurement

STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management & Budget
320 S. Walnut St, Lansing, MI 48933
P.O. Box 30026, Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **240000000752**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	Metrc
	4151 S. Pipkin Road
	Lakeland, Florida 33811
	Justin Green
	772-633-3240
	Justin.Green@metrc.com
	VS0039548

STATE	Program Manager	Various	LARA
		Phone Number	
		Email Address	
	Contract Administrator	Jeremy Lyon	DTMB
		517-230-2858	
		LyonJ5@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: LARA - Cannabis Regulatory Agency			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
5/7/2024	5/7/2029	5 – 1 year	N/A
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card	☐ Payment Request (PRC)	☐ Other	☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
New MA established from RFP# 230000003082. AD Board Approval 5/7/2024			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION		**1,923,000**	

Program Managers

Agency	Name	Phone	Email
LARA	Cole Thelen	517-388-8350	Thelenc10@michigan.gov
DTMB	Jason Wymer	517-2561014	wymerj@michigan.gov

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

____
Agency

____
Date

SOFTWARE CONTRACT TERMS AND CONDITIONS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this "Contract") are agreed to between the State of Michigan (the "**State**") and Metrc LLC, ("**Contractor**"), a Lakeland, Florida COMPANY. This Contract is effective on 5/7/2024 and unless terminated, will expire on 5/72029.

This Contract may be renewed for up to 5 additional 1-year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via a Change Notice.

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

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

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

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

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

"**Approved Third Party Components**" means all third party components, 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 Requirements.

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

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

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

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

"Change Notice" means a writing executed by the parties to the Contract memorializing a change to the Contract.

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

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

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

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

"**Contract**" has the meaning set forth in the preamble.

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

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor's Bid Response**" means the Contractor's proposal submitted in response to the RFP.

"**Contractor Hosted**" means the Hosted Services are provided by Contractor or one or more of its Permitted Subcontractors.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

“**Software**” means Contractor’s software as set forth in a Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract.

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

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

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

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

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

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

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

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

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

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

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

“System” has the meaning set forth in **Schedule I**.

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

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

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

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

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

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

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

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

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

“**User Data**” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, 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 90 calendar-day period commencing on the date of the State's Acceptance of the Software or System (if Contractor is providing Hardware under this Contract) for which Support Services are provided free of charge.

"**Work Product**" means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to Customizations, application programming interfaces, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

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

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

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

(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 Deliverables;

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

(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, each parties’ Contractor Administrator will sign a Change Notice**.**,

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

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

(ii) require Contractor to continue to negotiate a Change Notice;

(iii) initiate a Dispute Resolution Procedure; or

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

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

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

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

2.3 Contractor Personnel.

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

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

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

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

(iii) Contractor shall perform pre-employment background checks on all Contractor Personnel in accordance with Contractor's company policy Certification of performance of such background check and certification of passing results in accordance with Contractor's company policy must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. If, in its sole discretion, the State finds it reasonably necessary to perform its own background check, the State may also perform background checks. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

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

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

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

(a) Contractor Project Manager must:

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

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

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

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

(c) To the extent reasonably possible, Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless otherwise agreed by the Parties in writing through a Change Notice.

(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 or Contractor Project Manager has transitioned to a different role with Contractor.

(d) Upon the occurrence of any event set forth in **Subsections 2.4(c)(i-iii)** above, Contractor and State will meet to determine an acceptable resolution to both State and Contractor.

2.5 Contractor's Key Personnel.

(a) The State shall have the ability to provide feedback with regard to 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. At anytime during the Term that either the State or Contractor seeks a change in Key Personnel, the State and Contractor shall meet to reach a mutually acceptable resolution.

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

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

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

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

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

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

If to State:	If to Contractor:
Jeremy Lyon 320 S Walnut Street Lansing, MI 48933 LyonJ5@michigan.gov 517-230-2858	[Name] [Street Address] [City, State, Zip] [Email] [Phone]

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

5. Software License.

5.1 Perpetual License. RESERVED

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

(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 governmental purposes, including for Processing State Data;

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

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

(iv) access and use the Software for all such non-production uses and applications as may be necessary or useful for the effective use of the Software hereunder, including for purposes of analysis, development, configuration, integration, testing, training, maintenance, support and repair, which access and use will be without charge and not included for any purpose in any calculation of the State's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Subsection 5.2(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.** 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. State has the right to request disclosure of new Third Party Components, and Contractor will provide the State with information identifying and describing the addition within 30 days of the request. 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 **Subsection 7.1(c):**

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

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

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

8. Software Implementation.

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

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

9. Software Acceptance Testing.

9.1 Acceptance Testing.

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

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

(i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

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

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

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

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within 15 Business Days following the completion of any Acceptance Tests, including any Integration

Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Nonconformity in the tested Software.

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

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

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

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

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

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

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

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

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

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

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

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

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

10. Non-Software Acceptance.

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

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

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

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

10.5 If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may provide the non-Software Deliverables and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

11. Assignment. Contractor may not assign this Contract or any of its rights or delegate any of its duties or obligations hereunder, voluntarily, or involuntarily, whether by merger (regardless of whether it is the surviving or disappearing entity), conversion, consolidation, dissolution, or operation of law to any other party without the prior written approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other governmental entity if such assignment is made reasonably necessary by operation of controlling law or regulation. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

12. Change of Control. Contractor will notify the State, within 30 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 Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

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

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

13.4 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to 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 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 to be paid by the State 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 Schedule.

14. Liquidated Damages in the form of Service Level Credits.

14.1The parties understand and agree that any liquidated damages (which consist of those certain credits described and which are expressly for in Schedule D to 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 such liquidated damages for more than one event.

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

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

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

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

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

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

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

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

i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;

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

(iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

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

(i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

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

(c) The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must promptly reimburse to the State any

Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

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

(a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

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

16.3 Transition Responsibilities.

(a) Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 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**, including without limitation, the return or destruction of State Data at the conclusion of the Transition Period; and

(iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

(b) Contractor will follow the transition plan attached as **Schedule G** as it pertains to both transition in and transition out activities.

17. Indemnification

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

(a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;

(b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;

(c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable)~~;~~ and

(d) any intentional or willful acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

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

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding;

(c) employ its own counsel; and to

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

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

18. Infringement Remedies.

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

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

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

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

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

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

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

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

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

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

19. Disclaimer of Damages and Limitation of Liability.

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

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

20. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State as soon as reasonably practicable, in no case to exceed 30 calendar days, of receiving notice of material litigation that could effect Contractor's current or future ability to perform under the Contract (collectively, "Proceeding"), 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, mine, distribute, commercially exploit, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. Contractor's misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795.

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

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

(a) notify the State as soon as practicable but no later than 24 hours of becoming aware of such occurrence;

(b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;

(c) in the case of PII or PHI, at the State's sole election:

> (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or
>
> (ii) reimburse the State for any costs in notifying the affected individuals;

(d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;

(e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

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

(h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and

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

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

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

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

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

(a) the subcontractor is a Permitted Subcontractor;

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

(c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any of the Contractor's and Permitted Subcontractor's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Subsection 22.2**.

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

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

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

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

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

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

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

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

(a) Free of charge during the Warranty Period.

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

25. Data Security Requirements. Throughout the Term and at all times in connection 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 the Deliverable provided hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State's request, Contractor will timely provide training for additional Authorized Users or other additional training on the Deliverables for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

27. Maintenance Releases; New Versions

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

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

27.3 Installation. The State has no obligation to turn on or use any new features or functionality.

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

27.5 Additional functionality. Additional functionality, beyond that which is described in an existing Statement of Work will be added through the Change Control process.

28. Source Code Escrow

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

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

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

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

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

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

(i) conflict with or violate any applicable law;

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

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

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

(j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function 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. Conflicts and Ethics. Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract;

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

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

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

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

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

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

36. Force Majeure

36.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

36.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of 5 Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

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

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

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

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

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

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

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

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

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

41. Survival. Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification; disclaimer of damages and limitations of liability; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

42. Administrative Fee and Reporting

Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract for transactions with MiDEAL members and other states (including governmental subdivisions and authorized entities). For clarity, Contractor will not be obligated to pay an additional 1% administrative fee for payments made to the Contractor under the Contract for transactions with the State itself. Administrative fee payments must be made online by check or credit card at: https://www.thepayplace.com/mi/dtmb/adminfee.

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

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

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

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

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

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

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

45. 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.

46. Accessibility Requirements.

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

(a) maintain compliance with the Digital Accessibility Standards. ;

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

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

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

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

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

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

46.3 Warranty. Contractor warrants that all Digital Accessibility Standards 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 Digital Accessibility Standards conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in addition to all other remedies available to the State, the State may terminate this Contract for cause under **Subsection 16.1**.

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

46.5 Failure to comply with the requirements in this **Section 46** shall constitute a material breach of this Contract.

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

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

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

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

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

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

> (a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and
>
> (b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

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

Schedule A	Statement of Work
Schedule B	Pricing Schedule
Schedule C	Insurance Schedule
Schedule D	Service Level Agreement
Schedule E	Data Security Requirements
Schedule F	Disaster Recovery Plan
Schedule G	Transition Plan

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

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

SCHEDULE A – STATEMENT OF WORK

1. DEFINITIONS

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

Term	Definition
Solution	Deliverables (including but not limited to Software, Hardware, and Documentation) and Services (including but not limited to Hosting Services, Support Services), singularly or in any combination thereof as set forth in a Statement of Work intended to address the State's needs.
CRA	Cannabis Regulatory Agency
Provider	means a third-party system provider approved by the State to integrate with the statewide monitoring system required by the MMFLA, MTA, and MRTMA
Public Users	Owners and their designated staff that have access to the seed to sale system to make changes and upload daily transactions, transfers, or other necessary items to remain in compliance with the State of Michigan.

2. BACKGROUND

The State of Michigan (State), through the Cannabis Regulatory Agency (CRA) ("the Client"), has issued this RFP to obtain proposals from qualified firms for a vendor-hosted, web-based Software as a Service (SaaS) application that supports the identification and tracking of cannabis in all its forms. This statewide monitoring system is for the express purposes of collecting, reviewing and analyzing all data needed to effectively manage the Michigan Cannabis Rules as applicable for the State of Michigan. It will provide the needed accountability and controls required to protect the health and well-being of the population of the State of Michigan.

3. PURPOSE

The State is seeking either a Contractor Hosted or State Hosted Software Solution and applicable services. The State is contracting to acquire a fully developed software solution. The State is seeking a Commercial-Off-the-Shelf Software (COTS) solution with configuration changes as needed and/or Software as a Service (SaaS). The State is not seeking a fully custom designed system.

This contract is for *a Contractor Hosted* Software Solution and applicable Services

Term of the Agreement: 5 base years with 5 – 1 year options.

4. IT ENVIRONMENT RESPOSIBILITIES

Contractor will meet all Service Level Agreement requirements pertaining to Schedule D.

Contractors System will meet the requirements of Schedule D Service Level Agreement (SLA) is based on our use of an industry-accepted, best-practices-based approach to availability management.

For a Contractor Hosted Software Solution:

Definitions:

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

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

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

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

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

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

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

Component Matrix	Name all contractor(s) and/or subcontractor(s) providing each contract component
Facilities	Metrc
Infrastructure	Metrc
Platform	Metrc
Application	Metrc
Storage	Metrc
Backup	Metrc
Development	Metrc

5. ADA COMPLIANCE

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

6. USER TYPE AND CAPACITY

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

Type of User	Access Type	Number of Users	Number of Concurrent Users
Public users	Vendor employee will be restricted by write.	10,000	10,000
State Employee	Write, and Administrative	200	200
Provider	Vendor employee will be restricted by write.	250	250

Contractor will be able to support these response times with CRA's expected user count based on the provided user-count numbers.

7. ACCESS CONTROL AND AUTHENTICATION

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

To support federation with the SOM MILogin solution, the Contractor's solution must support SAML, OpenID or OAuth federated identity protocols.

Solutions running within the States internally managed IT environment may be suitable for integration with the State's Active Directory services as identified in the 1340.00.020.08 standard.

8. DATA RETENTION AND REMOVAL

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

The Solution allows the State to delete data, even data that may be stored off-line or in backups.

The Solution allows the State to retrieve data, even data that may be stored off-line or in backups.

The Contractor's System will allow CRA to retain all data for the entire length of the Contract.

The following default retention policy is applied to non-data storing components unless CRA requests an alternative, which can include retention up to 10 years:

- Backup Frequency – Daily
- Instant Restore – Retain instant recovery snapshots for 2 days
- Retention of daily backup point – Retain backup taken every day for 30 Days
- Retention of weekly backup point – Retain backup taken every week for 5 Weeks
- Retention of monthly backup point – Retain backup taken every month for 12 Month)

The following default retention policy is applied to systems that contain client data unless the state requests an alternative which can include data retention up to 10 years:

- Backup Frequency – Differential Every 12 hours
- Point in Time Restore – Retain PITR service for 7 days
- Retention of weekly full backup point – Retain backup taken every week for 12 Weeks

- Retention of monthly full backup point – Retain backup taken every month for 24 Months
- Retention of yearly full backup point – Retain backup taken every year for 7 Years

Data Deletion

The Contractors System does not allow CRA or any other users, including Contractors staff, to delete data, even data that may be stored off-line or in backups.

Data Retrieval

The Contractors System allows CRA to retrieve data, even data that may be stored off-line or in backups. The Contractors System maintains data for seven years. All data is retained in the System's primary operational database, allowing users to continue accessing the data (subject to user role permissions and other functional restrictions) for that entire period.

Data Management

The Contractors System stores all data, reports, forms, and images on the secured hosted infrastructure using encryption at rest. The database capacity within the Contractors System is essentially unlimited; databases can be sized up to 100TB.

9. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes currently supported versions of X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM, with supporting platforms, enterprise storage, monitoring, and management running in house and in cloud hosting provides.

Contractor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers and the state standard browser without the use of special plug-ins or extensions. The rules used to base the minimum browser requirements include:

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

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

Prior to making any changes in any environment, Contractor will discuss with the State project team. If necessary, these discussions can be escalated to project stakeholders for a final decision on whether to move forward with changes. After all discussions take place and an agreement is reached, agreed upon changes are started. Contractor will not make any changes without directly consulting with the State. If necessary, changes are defined using a change request and may, depending on the change, result in a contract amendment.

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.

Mobile Responsiveness

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

SOM IT Environment Access

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

- State provided VDI (Virtual Desktop Infrastructure) were 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 jurisdictional territories.

The Contractors system is a cloud-based SaaS solution, designed, developed, and owned by Contractor. Contractor's careful attention to detail is found throughout the contractor System's technical engineering. Each part of the System's technical architecture comprises logical component layers. These individual technology components stack into a solution infrastructure and are grouped into Web Access, Application Processes, and Technical Services layers. Contractor's security policy, techniques, services, and processes are deployed across all layers.

Contractor will provide a fully operational seed-to-sale tracking system that will continue to meet your functional and technical requirements as well as a comprehensive support and training program for all users, a team of experts dedicated to developing enhancements, and ongoing maintenance to ensure CRA's instance of the Contractors System continues to meet changing needs over the lifetime of the contract.

11. INTEGRATION

Contractor must integrate their solution to the following technologies:

Current Technology	**Currently there is an API in place to transfer data from Accela to the seed to sale system. FTP for Treasury Files.**
Volume of Data	**5 Licenses per day approximate**
Format of the input & export files	API and FTP

Contractor will continue to integrate with CRA's Accela system where the Contractor System receives business license and patient status updates via our secure API. The Contractor System also has supported FTP for Sales and Wholesale Transfer data to support the Treasury File requirements.

12. MIGRATION

Contractor must migrate the data identified in the table below:

Current Technology	**SaaS via web portal**
Data Format relative to the database technology used.	**SQL Tables (Azure Platform)**
Number of data fields to give Contractor awareness of the size of the schema.	**Hundreds**
Volume of Data	**Thousands of transactions daily.**
Database current size.	**Millions of Data Points**

The Contractor System is already operational in Michigan, we do not anticipate needing to provide data migration services for the State.

The database may be increased at the time of transition, if required by the State.

13. HARDWARE

The State is seeking proposals that would provide for the State to obtain title to- or ownership of, the Hardware; or for the Contractor to retain title to- or ownership of, the Hardware. Please provide one or both proposals for the State's consideration.

Contractor will provide the following Hardware:

Name of Hardware or Description	Quantity
RFID Handheld Readers	7-10

Contractor currently provides the CRA with handheld tag readers to support its field audits and investigations. CRA can purchase additional readers from Contractor.

Every handheld reader purchased through Contractor includes the following:

- Pre-installed, fully configured software (handheld app) that has already been tested, so the unit is ready to use right out of the box.
- Seamless integration with the Contractor System.
- Software and device training and support, including documentation for all partner users.
- Replacement of damaged units or parts, as covered by warranty.
- Repair of damaged units or parts, as covered by warranty.
- Replacement of outdated devices and software (additional detail below).

14. TRAINING SERVICES

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

Training Program is designed to ensure that CRA and licensee users can work proficiently in the Contractor System.

The following sections include:

- Training Process Flow
- Course Descriptions
- Competency Testing
- Training Materials
- Metrc Learn

Deliverable number	Deliverable specific
1	Develop a System User Manual, including system configurations for use by CRA staff.
2	Develop a System User Manual for industry users specific to the state regulations
3	Provide online training modules for all users (CRA staff and industry).
4	Train CRA staff not less than annually on basic and advanced use of the system and specifically identifying areas and flags where there are gaps in the system where inversion or diversion can happen.
5	Train CRA data analysts on the use of the Metrc data warehouse and update CRA staff when changes are made to the existing data dictionary, the data dictionary should be

	provided upon signing of the contract and not less than annually unless changes are made.
6	Provide technical training to CRA staff onsite 3 days minimum annually with the option to have an additional training if needed. This will include the following: using the system for enforcement including at a minimum: overview of the system, reports, and RFID scanners.
7	Provide a comprehensive state specific training plan for both state and industry users.

15. TRANSITION RESPONSIBILITIES

Please see Transition In and Out Plan in schedule G.

16. 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.

CRA and licensee users will have access to the following training materials to supplement and support their ability to use the System proficiently and with ease.

Content	Media	Delivery	Time Frame
Manual/User Guide	Printable PDF	Online through License	Provided to CRA & licensees at the time of contract
Knowledge Base	Online and Printable	Online through License	Available upon login

Up to 25 Quick Reference Guides	Online and Printable	Online through License	Metrc will create and maintain up to 25 Quick Reference Guides at the direction of the CRA. These guides will provide commonly requested information in a how-to format.
Industry Reports Guide	Printable PDF	Online through License	Provided to CRA & licensees at the time of credentialing
Testing Facility User Guide	Printable PDF	Online through License	Provided to Testing Facilities after Advanced Testing Facility Training
RFID Handheld Device Guide	Printable PDF	Online through License	Available to CRA upon request
CSV Industry Guide	Printable PDF	Online through License	Available to CRA & licensees at the time of credentialing
Industry Training Knowledge Checks (quizzes)	Online/On Demand	Online	Given via Metrc Learn upon completion of the New Business Training
Support Portal	Online/Email/Printable/Phone	Available Online/Phone	Provided at time of contract
Metrc Learn (LMS)	Online/On Demand	Available Online	Provided at the time of credentialing
Admin System Updates	PDF Bulletin/Printable	Available Online/Through License	Provided as updates are made in the System

Third-Party API Documentation	Online	https://api-ma.metrc.com/documentation	Currently available and ready to reference

17. Reserved - ADDITIONAL PRODUCTS AND SERVICES

18. CONTRACTOR PERSONNEL

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

Contractor
Name – Andrea Kiehl, Chief People & Legal Officer **Address – 4151 S. Pipkin Road, Lakeland, Florida 33811** **Phone – 819-433-7172** **Email – Andrea.Kiehl@metrc.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 – Joey Perdomo **Address – 3111 W Pipkin Rd, Lakeland, FL** **Phone – 1-877-566-6506** **Email – infosec@metrc.com**

19. CONTRACTOR KEY PERSONNEL

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

Contractor
Name – Brandon Zastrow, Customer Success Manager **Address – 4151 A Pipkin Road, Lakeland, Florida 33811** **Phone – 651-301-5692** **Email – brandon.zastrow@metrc.com**

20. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks. Upon request, Metrc will provide certification of passing background checks for Key Personnel to this project to the State of Michigan Program Manager designated for this Contract. In addition, proposed Contractor personnel will be required to complete a Michigan State Police background check and/or submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC), if required by project.

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

Contractor is based in Lakeland, Florida, and all tasks related to CRA's program will be performed inside the U.S. Contractor will not use offshore development services, and all System data will be stored within the U.S.

Disclosure of Subcontractors. If the Contractor intends to utilize subcontractors, the Contractor must disclose the following:

- The legal business name; address; telephone number; a description of subcontractor’s organization and the services it will provide; and information concerning subcontractor’s ability to provide the Contract Activities.
- The relationship of the subcontractor to the Contractor.
- Whether the Contractor has a previous working experience with the subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Contract Activities that will be performed or provided by the subcontractor.
- Geographically Disadvantage Business Enterprise Sub-Contractors: If the Contractors plan to utilize Subcontractors to perform more the 20% of the deliverables under this Contract, at least 20% of that Subcontractors work must be awarded to Michigan-based Geographically Disadvantaged Business Enterprises (GDBE). Contractor will submit a plan detailing all Subcontractors to be used, including the percentage of the work to be done by each. Contractor must inform the State to the name and address of the GDBE, the percentage of the work they will complete, the total amount estimated to be paid to the GDBE, and provide evidence for their qualifications as a GDBE. If Contractor cannot find GDBE Subcontractors to meet this requirement they must provide reasoning and justification to receive an exemption from this requirement from the State. (Existing business relationships will not be an approved reason for this.)

GDBE definition: "Geographically-Disadvantaged Business Enterprise" means a person or entity that satisfies one or more of the following: (i) Is certified as a HUBZone Small Business Concern by the United States Small Business Administration. (ii) Has a principal place of business located within a Qualified Opportunity Zone within Michigan. (iii) More than half of its employees have a principal residence located within a Qualified Opportunity Zone within Michigan, or both.

Additional information on GDBEs can be found here:

Michigan Qualified Opportunity Zone (QOZ) Map

Michigan Supplier Community (MiSC) Page

Contractor does not intend to use subcontractors for CRA's project.

21. STATE RESOURCES/RESPONSIBILITIES

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

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

State Contract Administrator
Name – Jeremy Lyon **Phone – 517-230-2858** **Email – LyonJ5@michigan.gov**

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

DTMB Program Manager
Name - Jason Wymer **Phone – 517-256-1014** **Email – Wymerj@michigan.gov**

Agency Program Manager
Name – Cole Thelen **Phone – 517-388-8350** **Email - ThelenC10@michigan.gov**

22. MEETINGS

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

1. Kick off meeting
2. Project planning sessions
3. SUITE tailoring sessions
4. Discovery/Requirements and analysis meetings
5. Ongoing collaborative team meetings to facilitate discovery and development are required. If Agile Scrum development approach is proposed, then all Scrum ceremonies,

including daily Scrum, sprint planning, sprint reviews, sprint retrospectives, backlog grooming, and artifacts will be encouraged and expected.

6. All other meetings needed to successfully implement the new system.
7. Daily standup/JAD sessions, depending on approach
8. Security plan assessment and review sessions

Contractor will attend all the meetings (1-8) set forth above at a location and time as identified by the State at no additional cost to the State.

Following go-live, Contractor will facilitate monthly meetings (or more/less if determined necessary by the parties) to ensure ongoing support success. CRA's assigned CSM will be in consistent and regular contact with CRA for agreed-upon dates, times, and frequency meetings with status reporting updates.

23. 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.

All Contractors must submit and enter weekly timesheets into the State of Michigan's Project Portfolio Management tool, Clarity PPM, for approval and reporting. The weekly Clarity PPM timesheet will contain hours worked for assigned project tasks.

We are highly collaborative and will work closely with CRA to ensure that the provided materials are in an approved format and provide all the information CRA desires. Weekly and monthly status reports will include the following:

- Project status summary
- Project status summary calculation tool
- Progress to complete milestones
- Percent complete
- Tasks and accomplishments completed last period
- Tasks planned for next period
- Open issues summary
- Open risks summary
- Open change requests
- Key performance indicators (KPIs)
- Key deliverables and milestones
- Time spent and action items accomplished each week

Contractor will also provide monthly reports to CRA that include System updates, changes, support data, information on all releases, summarized data on training attendance and support cases, and System performance information.

Contractor will provide a quarterly report once the implementation is complete and every quarter thereafter for the duration of our contract.

24. PROJECT MANAGEMENT

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

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

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.

Contractor will use the state of Michigan's SUITE templates for required documents, with the exception of some Contractor-developed documents. The Contractor-developed documents we are proposing to use are as follows:

- Defect Tracking Log (see Attachment H - Contractor UAT Defect Log)
- Maintenance Plan (see Attachment I - Contractor Maintenance and Operations Plan)
- Requirements Traceability Matrix (see Attachment J - Contractor MI Fit Gap Analysis)
- Requirements Specifications (see Attachment K - Contractor Requirements Specifications)
- Test Strategy (see Attachment L - Contractor Testing Approach)
- Use Cases (see Attachment M - Contractor State Configuration Primer)
- Detailed Test Plan (see Attachment N - Contractor UAT Test Plan)
- Test Case (see Attachment O - Contractor Sample Test Script)
- Test Closure Report (see Attachment P - Contractor UAT Closeout Report)
- Training Plan (see Attachment Q - Contractor Training Plan)

Milestones/Deliverables for Implementation

The State's proposed milestone schedule and associated deliverables are set forth below.

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

Contractor did not indicate any alternative timeframes or deliverables are necessary and indicated the timeline set above is feasible.

25. HUMAN CENTERED DESIGN (HCD)

The State intends to utilize Human Center Design as an option to increase stakeholder engagement and to improve state services. The Contractor may deploy specific activities to; garner stakeholder input, define needs, understand issues; facilitate ideation, facilitate prototype creation, set metrics/measures, and recommend a program of change. The Contractor may engage in ongoing feedback with stakeholders through the implementation of recommended change. These activities should be reflected in your pricing structure.

Contractor will focus our Human Center Design (HCD) efforts on engaging in ongoing feedback from stakeholders about their experience of the Contractor System.

NOTE: If proposed, please ensure your pricing and project schedule reflect a line item for the HCD components proposed, specific to each deliverable and tool used (research and design).

26. ADDITIONAL INFORMATION

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

SCHEDULE A – TABLE 1 – BUSINESS SPECIFICATION WORKSHEET

A	B
Business Specification Number	**Business Specification**
REQUIRED	
1.0	The system must provide an integrated marihuana tracking, inventory and verification system.
2.0	The system must have the capability of storing data. Data storage will be included in the contract for documents.
3.0	The system must have capability of providing access to data. This includes but is not limited to a data map, as well as access to all pertinent tables for the purpose of legislative requirements and enforcement of the pertinent rules.

4.0	The system must allow authorized law enforcement agencies with the proper access to verify the registry ID card of a patient or primary caregiver is valid and current.
5.0	The system must allow authorized auditors access to the system in order to conduct periodic audits of all marihuana facilities.
6.0	The system must have the capability of receiving data.
7.0	The system must have the capability of integrating data.
8.0	The system must be made available to all authorized users 24X7X365.
9.0	The vendor will provide training including but not limited to online tutorials, annual training, and training prior to access to the system. This is applicable to both the internal and external users.
10.0	The system shall use role-based security for system access and supported functionality.
11.0	The system must allow an authorized user the ability to create roles as needed.
12.0	The system must support the ability for an authorized user to associate individual users with one or more roles.

13.0	The system must support the ability for an authorized role to remove individual users from one or more roles.
14.0	The system must be able to support password changes without administrative or contractor interaction.
15.0	All data must be stored and maintained by the contractor.
16.0	The State must retain sole ownership of all data.
17.0	The contractor must provide any or all data upon request from the State.
18.0	Data collected by the system must be available for a defined period of time.
19.0	Data stored within the defined time period must be available for recall by users for data and/or public disclosure requests.
20.0	Following the defined retention, data must be archived to a mutually agreed upon permanent storage medium prior to removing it from the system.
21.0	The system must have the capability to support administratively maintainable business rules.
22.0	The system must allow the State to receive email system alerts based on administratively maintained business rules.

23.0	The system must allow the State to receive internal system alerts based on administratively maintained business rules.
24.0	Alerts must be configurable by an authorized user to set tolerance levels.
25.0	The system must send out notifications of changes to licensees.
26.0	Alerts must be configurable by an authorized user to select alert recipients.
27.0	Email alerts must be triggered by tracking events which are outside of tolerance levels. Alerts sent to customer and specified email address at CRA
28.0	The amount authorized to be purchased must be a configurable value.
29.0	The system must contain a robust search mechanism for look ups.
30.0	The system must support keyword lookups.
31.0	The system must contain search functionality to allow authorized users to search inventory items by entering a set of search criteria and displaying the results in a tabular form.
32.0	All licensed authorized users must have the capability to access the system through a secure Application Programming Interface (API) web interface for data entry, data upload, data display and reporting.

33.0	The system must include a certification and testing program to ensure that all licensees can demonstrate the capability to correctly use the secure data connection interface before they are authorized to submit data to the system.
34.0	The system must allow all licensed authorized users the capability to manually enter data into input screens.
35.0	The system must allow authorized users the capability to edit or correct data before posting to the system.
36.0	The interface must allow an authorized user to enter information in the system.
37.0	The interface must allow an authorized user to access information in the system.
38.0	The interface must allow real time access by all authorized personnel.
39.0	The system must have the capability to electronically receive and store information in a centralized database.
40.0	The system must have the capability to electronically transmit information.
41.0	Data input must include, but is not limited to the following fields: · Receipt date · Received by (licensee)

	· Employee · Source licensee name · Source license number · Order number · Items shipped or received · Product ID (unique identifier) · Product name · Lot number · Batch number · Weight · Quantity
42.0	Data Available for reporting must include but is not limited to the following fields: Package ID Package Quantity Sales Quantity Sales Total Sales Delivery Package Weight Product Weight Product Type Product Item Weight (for individual items)

	Product Volume Package Volume Package Facility Product Facility License Number Shipped Weight Shipped Volume Shipped Facility Package OnHold Package InTransit Package Finished Plant Growth Stage Plant Destroyed Plant Harvested
43.0	The system must track items in US customary and metric units.
44.0	The system must allow authorized users to track transfers from a registered primary caregiver to a Laboratory for testing.
45.0	The system must allow an authorized grower or employee of the grower to enter the following information into the statewide monitoring system via a secure web interface:

	· All transactions · Current inventory
46.0	The system must allow an authorized secure transporter or employee of the secure transporter to enter the following information into the statewide monitoring system via a secure web interface: · All transactions · Current inventory
47.0	The system must allow an authorized Laboratory user to enter the following information into the system. Input may include, but is not limited to the following: · All transactions · Current inventory All other required information as defined by the legislation.
48.0	The system must allow an authorized provisioning center licensee to enter all transactions into the system.
49.0	The system must allow an authorized provisioning center user to enter all current inventory into the system.
50.0	The system must allow an authorized user to indicate which requirements apply to which licensee type.

51.0	The system must allow an authorized user to maintain a list of different licensee types and their compliance requirements. - Grower - Processor - Laboratory - Provisioning center
52.0	The system must allow an authorized user to maintain a description of each licensee type.
53.0	The system must allow an authorized user to maintain a list of license classes.
54.0	The system must allow an authorized user to indicate the type of license class issued to a grower.
55.0	The system must allow an authorized user to maintain a name for each license class (i.e., “Class A”, “Class B”, etc.).
56.0	The system must allow an authorized user to maintain a description for each license class (i.e., “0-500 plants”, “501-1,000 plants”, etc.).
57.0	The system must maintain historical license associations with class and descriptions at time of issued license.
58.0	The system must maintain a historical association of license classes issued to a grower over time.

59.0	The system must establish an interface with the State of Michigan’s Accela system to extract information pertaining to the registered qualifying patient’s or registered primary caregiver’s identification card.
60.0	The system must have the capability to track all lot and batch information throughout the entire chain of custody. (i.e. from seed to sale).
61.0	The system must have the capability to be utilized as an inventory control system by tracking inventory control levels, orders, sales and deliveries.
62.0	The system must allow an authorized user to maintain a description of each licensee type.
63.0	The system must have the capability to track the product inventory which is available for sale.
64.0	The system must allow input, tracking, reporting and storage of information about marihuana and marihuana products received at a licensee facility from other licensees.
65.0	The system must have the capability of tracking all inventory discrepancies.
66.0	The system must assign a globally unique, non-repeating identification number for every plant and inventory item recorded in the system.
67.0	The system must have the capability to track, by unique identifier, all: - Marihuana plants

	- Marihuana derivatives - Marihuana packages
68.0	The system must have the capability to track all marihuana plant destruction and waste.
69.0	The system must have the capability to track all marihuana transfers
70.0	The system must have the capability to track all marihuana conversions from a processor.
71.0	The system must have the capability to track all marihuana and marihuana product returns.
72.0	The system must have the capability to track all products throughout the chain of custody.
73.0	The system must have the capability to track all conversions throughout the chain of custody.
74.0	The system must have the capability to track all derivatives throughout the chain of custody.
75.0	The system must have the capability to track all marihuana batch destruction.
76.0	The system must have the capability to perform batch recall tracking.
77.0	The system must have the capability to track the recall of the product sold.
78.0	The system must have the capability to track the product which is in the process of transfer for a product recall.

79.0	The system must have the capability to track the product which is being processed into another form for a product recall.
80.0	The system must have the capability to track postharvest raw product which is in the drying process for a product recall.
81.0	The system must have the capability to track postharvest raw product which is in the trimming process for a product recall.
82.0	The system must have the capability to track postharvest raw product which is in the curing process for a product recall.
83.0	The system must have the capability of tracking the loss of a marihuana product.
84.0	The system must have the capability of tracking the theft of a marihuana product.
85.0	The system must track the sale or transfer of marihuana products (excluding seeds) to a processor.
86.0	The system must track the sale or transfer to a provisioning center of: - Marihuana plants - Marihuana derivatives - Marihuana packages
87.0	The system must have the capability to track all marihuana and marihuana product sales.

88.0	The system must have the capability to track all patient’s purchase totals, within a commercially reasonable time frame.
89.0	The system must have the capability to track all caregiver’s purchase totals within a commercially reasonable time frame
90.0	The system must have the capability of tracking adverse reactions for all consumers (Patients, Recreational, etc.)
91.0	The system must have the capability of tracking dose-related issues, including tracking THC and CBD to the individual item.
92.0	The system must have the capability of tracking all refunds.
93.0	The system must allow authorized users the capability to cross-check that product sales are made to a registered qualifying patient.
94.0	The system must allow authorized users the capability to cross-check that product sales are made to a registered primary caregiver.
95.0	The system must have the capability to track patient purchase limits.
96.0	The system must have the capability to track the per transaction limit per the Michigan Cannabis Regulations.

97.0	The system must verify to an authorized user the sale or transfer of marihuana to a registered qualified patient does not exceed the daily purchasing limit.
98.0	The system must verify to an authorized user the sale or transfer of marihuana to a registered primary caregiver does not exceed the daily purchasing limit.
99.0	The system must have the capability to flag the purchase of untested marihuana or marihuana products.
100.0	The system must provide the capability to retain the date of each sale of marihuana to a registered qualified patient.
101.0	The system must provide the capability to retain the date of each sale of marihuana to a registered primary caregiver.
102.0	The system must provide the capability to retain the date of each transfer of marihuana to a registered qualified patient.
103.0	The system must provide the capability to retain the date of each transfer of marihuana to a registered primary caregiver.
104.0	The system must provide the capability to retain the time of each sale of marihuana to a registered qualified patient.
105.0	The system must provide the capability to retain the time of each sale of marihuana to a registered primary caregiver.

106.0	The system must provide the capability to retain the time of each transfer of marihuana to a registered primary caregiver.
107.0	The system must provide the capability to retain the time of each transfer of marihuana to a registered qualified patient.
108.0	The system must provide the capability to retain the quantity of each sale of marihuana to a registered qualified patient.
109.0	The system must provide the capability to retain the quantity of each sale of marihuana to a registered primary caregiver.
110.0	The system must have the capability to track the quantity of each sale per the Michigan Cannabis Regulations.
111.0	The system must provide the capability to retain the quantity of each transfer of marihuana to a registered qualified patient.
112.0	The system must provide the capability to retain the quantity of each transfer of marihuana to a registered primary caregiver.
113.0	The system must provide the capability to retain the price of each sale of marihuana to a registered qualified patient.
114.0	The system must provide the capability to retain the price of each sale of marihuana to a registered primary caregiver

115.0	The system must provide the capability to retain the price of each transfer of marihuana to a registered qualified patient.
116.0	The system must provide the capability to retain the price of each transfer of marihuana to a registered primary caregiver.
117.0	The system must indicate to an authorized user whether the registered qualifying patient has a valid registry identification card.
118.0	The system must indicate to an authorized user whether the registered primary caregiver has a valid registry identification card.
119.0	The system must have the capability to track fees associated with the purchase or sale of marihuana between facilities.
120.0	The system must allow an authorized user the capability to enter a route plan into the system.
121.0	The system must have the capability to track all the transportation of all marihuana related products.
122.0	The system must allow an authorized user the capability to enter a route plan into the system.
123.0	The system must allow an authorized user to maintain a historical list of route plans and manifests.

124.0	The system must allow an authorized user to indicate that a laboratory has performed the required safety compliance tests.
125.0	The system must allow authorized users the capability to cross-check that the product received the required safety compliance testing.
126.0	The system must have the capability to administratively maintain a list of tests necessary to determine compliance as prescribed by the business rules.
127.0	The system must allow an authorized user to enter limits for test items.
128.0	The system must allow an authorized user to enter results against test items.
129.0	The system must allow an authorized user to maintain a list of chemical levels.
130.0	The system must allow an authorized user to maintain a description of each chemical level.
131.0	The system must allow authorized users the capability to link the testing results to each source batch.
132.0	The system must allow authorized users the capability to link the testing results to each sample.
133.0	The system must allow authorized users the capability to identify test results which may have been altered.

134.0	The system must have the capability to receive testing results from a Laboratory via a secured Application Program Interface (API).
135.0	The system must be accessible from mobile devices.
136.0	The system must have the capability to download and search datasets to create multiple reports utilizing the required data.
137.0	The system must provide ad-hoc reporting functionality for the State to determine compliance with Michigan statutes and rules.
138.0	The system must provide pre-defined reporting functionality for the State to determine compliance with Michigan statutes and rules
139.0	The system must allow the State to define new reports as needed without assistance or ongoing support from the contractor.
140.0	The system must allow the State to edit report formats as needed without assistance or ongoing support from the contractor.
141.0	The system must have the capability to produce electronic reports.
142.0	The system must have the capability to print electronic reports.
143.0	The system must allow an authorized user to select a pre-defined report of all inventory discrepancies for a particular location.

144.0	The system must allow an authorized user to select a pre-defined report on the loss of products containing marihuana.
145.0	The system must allow an authorized user to select a pre-defined report of all inventory discrepancies for a particular location.
146.0	The system must allow an authorized user to select a pre-defined report of all adverse patient responses.
147.0	The system must allow an authorized user to select a pre-defined report of all dose related issues.
148.0	The system must allow an authorized user to select a pre-defined report of all sales.
149.0	The system must allow an authorized user to select a pre-defined report of all marihuana and product refunds.
150.0	The system must allow an authorized user to select a pre-defined report on total daily sales.
151.0	The system must allow an authorized user to select a pre-defined report on the total number of marihuana plants in production.
152.0	The system must allow an authorized user to select a pre-defined report on the total number of marihuana plants destroyed.
153.0	The system must allow authorized users to select from a list the total inventory of marihuana adjustments report.

154.0	The system must provide a report on employee history (common employees between facilities/establishments).
155.0	The system must provide a report on license history for anomalous activity
156.0	The system must be able to provide the ability to determine which companies the largest transfers take place with and/or more adjustments/wasted product.
157.0	The system must allow for item brand functionality and Approval processes - Naming Conventions concern
158.0	The system must contain a field for manifests for invoice numbers
159.0	The system must have a more robust query tool that sits on top of the backend tables.
160.0	The system must allow for a user to create temp tables
161.0	The system must increase query run speed and/or open the system governor
162.0	The system must have a canned report that covers transfers by secure transporter
163.0	The system must contain a report that gives the user AU sales by receipt that calculated the total flower equivalent per receipt
164.0	Vendor must provide a Map of data structure

165.0	The system must allow an authorized user the ability to edit sales delivery receipts
166.0	The system must create a transfer type for money going to a third license
167.0	The system must allow for a Process for updating investigative samples to submitted for testing
168.0	The system must allow for batch file exports to sFTP for other state agencies or partners.
169.0	The system has to be capable of using the existing transfer types, and item categories currently established and any additional types that are required by rule.
170.0	The system has to be capable of tracking tolling agreements and have the ability to link a specific agreement to the transfer it applies. Explanation: This would be 3*rd* party agreements involving 2 or more licensees, such as grower A transfers biomass at no charge to processor B who will process it and ship it to processor C again no charge but there is an agreed upon percent of sales or amount per Liter of extracted material.
171.0	The system shall replicate database tables to the State’s Data Warehouse environment at least on a daily basis.

SCHEDULE B - PRICING

Price proposals must include all costs for the licensing,
support, implementation, and training for the Solution.

1. Licensing Fees. If Contractor is proposing a perpetual license, Contractor shall include the one-time cost of the license, which shall cover all intended users of the Solution (please refer to the estimated number and type of users identified in the **User Type and Capacity Section of Schedule A - Statement of Work**). If Contractor is proposing a term-based license, Bidder shall include annual costs for the term-based license for, which shall cover all intended users of the Solution (please refer to the estimated number and type of users identified in the **User Type and Capacity Section of Schedule A - Statement of Work)**. While the State is looking for precise pricing based on the estimated number of users, Contractor is encouraged to also provide a separate, tiered pricing structure to afford the State discounted pricing based on potential increases in volume in the future. If Bidder offers an enterprise pricing model (e.g. unlimited number of users), it is encouraged to separately provide that pricing option as well.

If Contractor is proposing a subscription License Model, only Table A must be completed. If Contractor is proposing a Perpetual License Model, License costs must be included in Table B.

2. Support Service Fees. The Contractor must identify any monthly costs for ongoing support of the Solution (the "**Support Service Fees**") to meet the requirements of **Schedule D to the Contract Terms** - **Service Level Agreement.** Separate Support Service fees must be documented in Table B below.

3. Hosting Fees. If Contractor is proposing a perpetual license with a separate hosting cost (direct or through a subcontractor), Contractor must provide the monthly hosting cost in Table B below. Contractor shall include the hosting costs to accommodate all intended users of the Solution (please refer to the estimated number and type of users identified in the **User Type and Capacity Section of Schedule A - Statement of Work**). Contractor must also provide tiered pricing for hosting to accommodate future growth or reductions.

Table A - Subscription License Model

Because Metrc is proposing a subscription license model, we have completed Table A and left Table B blank. Please note: State user support and hosting fees are included in the below pricing.

Subscription Based - Product Name	Annual License Subscription Fee (Price per user)	Annual Tiered Pricing	Annual Enterprise Licensing – Unlimited Number of Users
Metrc SaaS - Year 1	N/A	N/A	$112,000
Metrc SaaS - Year 2	N/A	N/A	$122,000
Metrc SaaS - Year 3	N/A	N/A	$137,000
Metrc SaaS - Year 4	N/A	N/A	$152,000
Metrc SaaS - Year 5	N/A	N/A	$172,000
Metrc SaaS - Year 6	N/A	N/A	$182,000
Metrc SaaS - Year 7	N/A	N/A	$192,000
Metrc SaaS - Year 8	N/A	N/A	$202,000
Metrc SaaS - Year 9	N/A	N/A	$212,000
Metrc SaaS - Year 10	N/A	N/A	$222,000
Spector App	$96	N/A	N/A

Table B – Perpetual License Model

Metrc is not proposing a perpetual license model and has left this table blank, per RFP instructions.

Licensing and Hosting costs will be paid after installation, configuration, and State testing and acceptance of the Solution.

The contract pricing for Support Fees will be awarded based on a firm fixed fee. However, for price evaluation purposes, Bidder must provide a breakdown of how Support Fees were calculated.

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

Bidder must provide detailed pricing and a payment schedule for the implementation of their product.

Metrc Implementation Fees: $200,000

Metrc calculated the implementation costs by estimating the level of effort (four sprints, eight weeks of development work) to deliver the requirements specified in this RFP that we determined "Require Customization," as noted in our response to the Business Specification Worksheet.

Implementation Fees will be awarded based on a firm fixed fee. However, for price evaluation purposes, Bidder must provide a detailed breakdown of how Implementation Fees were calculated.

5. Postproduction Warranty. The Contractor must provide a 90 calendar days postproduction warranty at no cost to the State. The postproduction warranty will meet

all requirements of the contract, including all Support Services identified in Schedule D.

While CRA did not specify the number of days for post-production warranty, Contractor looks forward to discussing coverage options.

6. Rate Card for Ancillary Professional Services.

Resource	On-Site Hourly Rate	Remote Rate
Product Owner	N/A	$150
Developer	N/A	$200
Quality Assurance (QA)	N/A	$100

Price proposals must include a fixed-price hourly-rate rate card for ancillary professional services (e.g. future enhancement configuration services) broken down by role (e.g. Solution design architect). If Bidder differentiates between on-site and remote services, provide pricing for both.

7. Open Source or Third Party Products

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

While Contractor does not require open-source or third-party products, there are certain components associated with Contractor System that are transacted directly between Contractor and industry licensees. Licensees will be responsible for compliance with Contractor's software requirements; these requirements include but are not limited to any subscription or transactional fees charged by Contractor . Contractor will be responsible for collecting such fees directly from licensees; the CRA will not be responsible for these costs. Contractor will provide these costs upon request.

Product	Price

8. Hardware Pricing

The Contractor must identify the hardware and pricing.

Product	Price
RFID Handheld Reader	$1,800

9. 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.

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

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

SCHEDULE C - INSURANCE REQUIREMENTS

Request For Proposal No. 230000003082
LARA - Cannabis Regulatory Agency

Contact DTMB Enterprise Risk Management at DTMB-RiskManagement@michigan.gov for 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	

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

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

STATE OF MICHIGAN
PROCUREMENT
Michigan.gov/MiProcurement

SCHEDULE D – SERVICE LEVEL AGREEMENT

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

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

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

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

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

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

"**Corrective Action Plan**" has the meaning set forth in **Subsection 3.9.**

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

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

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

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

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

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

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

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

"**Scheduled Downtime**" has the meaning set forth in **Subsection 2.3.**

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

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

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

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

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

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

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

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

"**Support Hours**" means 8 am to 5 pm Eastern, Monday - Friday.

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

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

2. Service Availability and Service Availably Credits.

2.1 Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a "**Service Period**"), at least 99.9% 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: (Actual Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) x 100 = Availability.

2.2 Exceptions. No period of Hosted Services 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 **Subsection 2.3.**

2.3 Scheduled Downtime. Contractor must notify the State at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services or Software in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

2.4 Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than three (3) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

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

2.6 Remedies for Service Availability Failures.

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

SERVICE AVAILABILITY TABLE

Availability	**Credit of Fees**
≥99.9%	None
<99.9% but ≥99.0%	15%
<99.0% but ≥95.0%	50%
<95.0%	100%

(b) Any Service Availability Credits due under this **Subsection** 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, the parties will make best efforts to agree to a remediation plan within ten (10) days. In addition to all other remedies available to the State, the State may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

3. Support and Maintenance Services. Contractor will provide Hosted Services, Software, and Hardware (if applicable) maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this **Section 3.** The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

3.1 Support Service Responsibilities. Contractor will:

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

(b) provide unlimited telephone support, 8 am to 5 pm, Monday – Friday Eastern standard time.

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

(d) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

(e) respond to and Resolve Support Requests as specified in this **Section 3.**

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

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

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

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

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

(ii) If Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Subsections 3.5 and 3.6**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

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

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

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

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

3.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 3** ("**Support Service Level Requirements**"), and the Contract.

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

SUPPORT REQUEST TABLE

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
Critical Service Error	• 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. • Hardware not operable
High Service Error	• Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	• Hosted Services and Software is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
	around.
Low Service Error	- Request for assistance, information, or services that are routine in nature.

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

RESPONSE AND RESOLUTION TIME SERVICE TABLE

Support Request Classification	**Service Level Metric** **(Required Response Time)**	**Service Level Metric** **(Required Resolution Time)**	**Service Level Credits** **(For Failure to Respond to any Support Request Within the Corresponding Response Time)**	**Service Level Credits** **(For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)**
Critical Service Error	One (1) hour	**For Hosted Services and Software**	Five percent (5%) of the Fees for the month in which the initial	Five percent (5%) of the Fees for the month in which the initial Service Level

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)
		Three (3) hours **For Hardware:** 1 business day	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.	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 corresponding Service Error is	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-Resolved, which amount will

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

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

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

3.9 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

4. Hardware.

When the Contractor receives calls for repair and/or replacement of Hardware, the Contractor must correct such problems within 1 Business Day of notification by the State. The Contractor must maintain sufficient inventory of spare equipment to meet the 1 Business Day requirement. Failure to repair or replace the Hardware within this timeframe will result in the assessment of liquidated damages of $100 per day until resolved.

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

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

5.2 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**.**

5.3 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.

5.4 Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 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 4;** and provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

BIDDER INSTRUCTIONS

Bidder must provide a current list of Contractor contacts and telephone numbers 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.

BIDDER RESPONSE:

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 Personnel comply with the foregoing.

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

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

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

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

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

5.3 ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, developed and backed up in the continental United States, and the data center(s) in which State Data resides minimally meets Uptime Institute Tier 3 standards (https://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 Throughout the Term, Contractor must not provide Hardware or Services from the list of excluded parties in the System for Award Management (SAM) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services.

5.6 provide technical and organizational safeguards against accidental, unlawful 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);

5.7 take all reasonable measures to:

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

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

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

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

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

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

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

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

8. Security Audits.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10. Infrastructure Scanning.

10.1 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 F – DISASTER RECOVERY PLAN

DISASTER RECOVERY & BUSINESS CONTINUITY PLAN

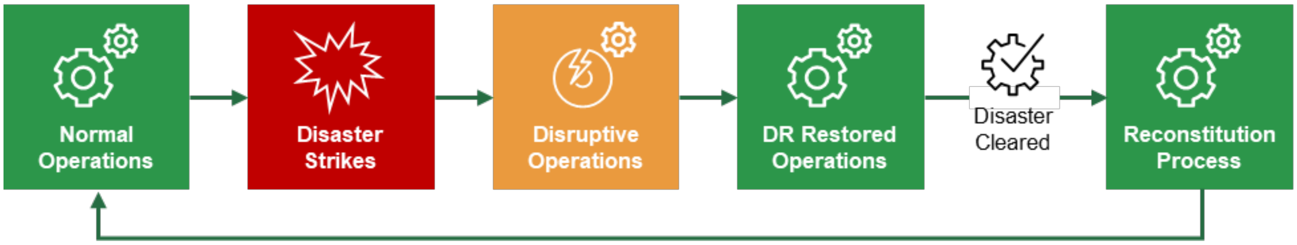
TABLE OF CONTENTS

OVERVIEW

This document serves as a dynamic and changing record of the on-going execution of the Disaster Recovery and Business Continuity policies associated with the Metrc System. The intended purpose is to have a clearly documented understanding of the Metrc System infrastructure and a plan for disaster recovery, system resiliency, and data loss protection.

DISASTER RECOVERY LIFE CYCLE

Disasters are unpredictable but should be considered expected from a planning viewpoint. The cycle of disaster recovery stages illustrates that the goal of disaster recovery is to return operation of the Metrc solution and its supporting services back to their normal production status. Additionally, it highlights that during a disaster, there will be some disruption. Thoughtful design and careful planning help Metrc mitigate the risk of disruption and reduce the duration of the disruption when it does happen.



Disaster Recovery Life Cycle

NORMAL OPERATIONS

This stage is the desired normal production status of the Metrc System and its supporting services.

DISASTER STRIKES

CRISIS MANAGEMENT	Disaster Occurs	The production datacenter site has been impacted by a disaster disrupting production Metrc servers or databases.
	Detection of Disaster	Notification comes in via report, monitoring tools, or directly from our infrastructure provider.
	Triage	The Emergency Response Team will need to assess damage and perform triage on the impact on the disaster.

	Communication	Provide external communication on impact and current stage of Disaster Recover Life Cycle.

DISRUPTIVE OPERATIONS

This stage represents the status of Metrc or a support service after a disaster has struck. For a major incident like a tornado, this could represent complete downtime of the Metrc solution. A minor incident such as a server failure would merely require switching workload to a hot-standby secondary server and would reduce the impact of disruptive operations.

DR RESTORED OPERATIONS

This is the stage where recovery activities begin and service is brought back to an acceptable running status. For a major incident, this might require switching workload and traffic to a secondary datacenter. A minor incident might be successfully restored by switching to secondary equipment that can then become the new production equipment.

RECOVERY	Verify Capabilities	Verify extent of impact on production servers.
	Data Integrity Audit	Conduct assessment of data integrity in Disaster Recovery (DR) servers. Ensure data replication is satisfactory. Assess compliance with Recovery Point Objectives are outlined in our Metrc Standard Service Level Agreements document.
	DR Web Servers	Configure and validate functionality of web servers within DR data center.
	DR Load Balancers	Configure and validate functionality of load balancers within DR data center.

	DNS Configuration	Update DNS configuration to deployment as needed. Verify Cloudflare deployments failover. Address any deployments that require manual configuration of IP addresses in infrastructure provider console. Confirm the successful propagation of the updated DNS records.
	Limitation of Resources	Only enable necessary resources to allow for limited disaster recovery operation.

	Smoke Testing	Bring up relevant systems and application supporting services in the environment. Verify via internal testing that each deployment is correctly deployed. Verify that the Metrc application is available and offers the expected functionality and performance.
	Communication	Provide external communication on impact and current stage of Disaster Recover Life Cycle.

RECONSTITUTION PROCESS

In this stage, operations are transferred back to the original system or facility. If the original system or facility is not recoverable, this phase also involves rebuilding. Rebuilding is the process of establishing a new facility/equipment to replace what was destroyed and no longer operational. During rebuilding, the backup data center that is acting as production will not have a backup data center; however, backups of the Metrc databases would still be performed.

RECONSTITUTION	Reestablish Secondary Location	After scaling up DR server infrastructure, the reestablishment of a secondary data center location is necessary. Ideally the original production location would be able to be the new Secondary location. Otherwise, the organization will evaluate and select a new secondary location.
	Validate and Evaluate	Perform all relevant Reconstruction stage activities on the newly established location.
	Communication	Provide external communication on impact and current stage of Disaster Recover Life Cycle.

RESUMPTION OF NORMAL OPERATIONS

This stage is the return to desired normal production status of the Metrc System and its supporting services.

RESUMPTION	Return to Original Operations	Evaluate and approve that original production location is ready to resume production operation. If unable to resume original operations, the organization will evaluate and approve a new Production and DR locations.

	Validate and Evaluate	Perform all of the Recovery stage activities on the newly established location.
	Communication	Provide external communication on impact and current stage of Disaster Recover Life Cycle.

PLAN ACTIVATION TRIGGER

The Disaster Recovery Plan should be activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority should activate the plan.

Activation criteria for system outages or disruptions are as follows:

- Extent of any damage to the system (e.g., physical, operational, or cost) exceeds thresholds.
- Failure of a system deemed a critical infrastructure production asset impacting the organization’s mission.
- Expected duration of the outage lasting longer than the RTO.

DISASTER RECOVERY COMMUNICATION

In the event of a critical incident, disaster or catastrophic failure that results in significant data loss or extended access loss, Metrc will meet the requirements of Disaster Recovery and Business Continuity as follows:

- Communicate nature of impact and limited access during Recovery and Reconstitution stages of Disaster Recovery Lifecycle.
- Provide timely updates on impact, changes, and timeline for progress.
- Promptly notify delegate in writing of any data breach.

DISASTER NOTIFICATION

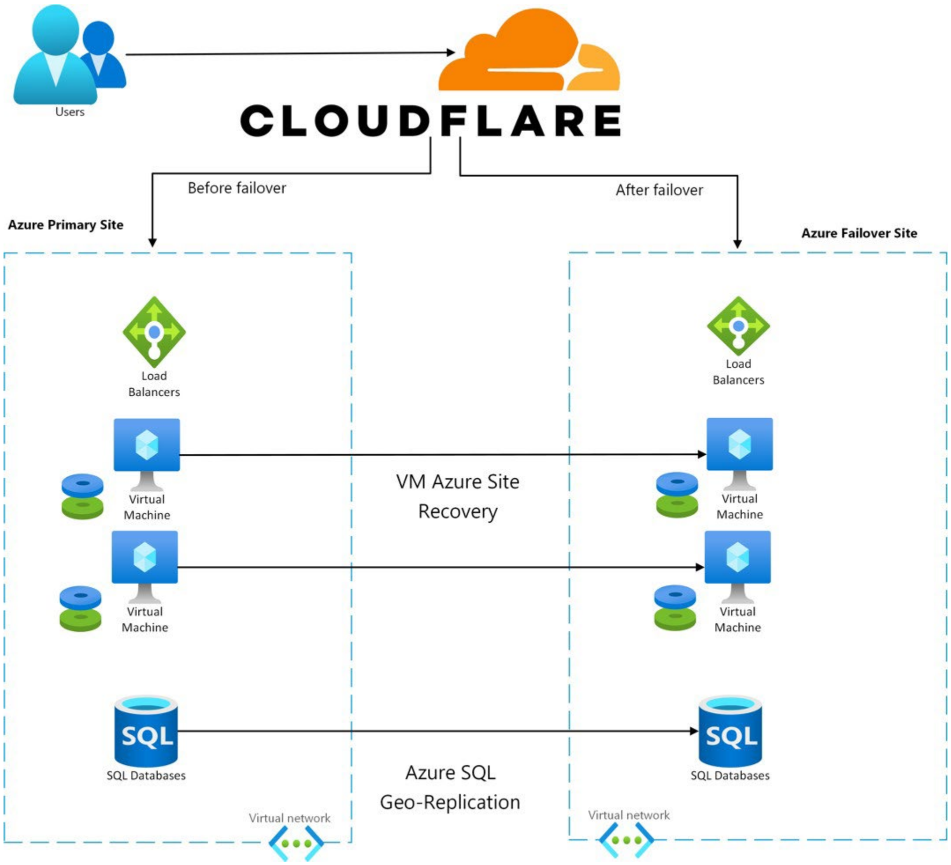
First, we immediately notify the designee by the fastest method possible in writing. Metrc will provide such notification within twenty-four (24) hours after we reasonably believe there has been a disaster or catastrophic failure. This notification will include:

- The scale and quantity of data affected.
- The actions Metrc has taken, or will take, to recovery the data.
- The corrective actions Metrc has taken, or will take, to prevent future data loss

Second, simultaneously, we restore continuity of Metrc, restore data in accordance with the RPO and RTO as set forth in the SLA, restore data accessibility, and repair Metrc as needed to meet SLA performance requirements.

Finally, we investigate the disaster or catastrophic failure and share the results report with the State. Metrc agrees that the State and/or its agents will have the right to lead (if required by law) or participate in the investigation. Metrc will cooperate fully with the State, its agents, and law enforcement.

INFRASTRUCTURE DIAGRAM



INFRASTRUCTURE DESIGN

The Metrc System infrastructure consists of highly available and geo-redundant architecture consisting of a Production datacenter site and a Disaster Recovery (DR) datacenter site. These sites are linked via a cross- region replication. Metrc achieves resiliency for the Metrc System infrastructure by focusing our design on high availability server clusters. This is ensured by scheduling portions of each cluster for preventive operations on cascading intervals allowing for minimal down time and maximum availability. Metrc leverages industry best practices to design and provide the Metrc System as a highly resilient solution that will meet and often exceed 99.97% availability.

GEO-REDUNDANCY

The Production datacenter site is located in Illinois and the DR datacenter site is in Texas. These sites are geographically distinct to ensure a minimum distance of 500 miles between datacenter sites. Datacenter site separation reduces the likelihood that natural disasters, civil unrest, power outages, or physical network outages can affect the availability of the Metrc System due to redundancy.

Redundancy is the duplication of critical system components or functions with the intention of increasing reliability by reducing single points of failure through the implementation of backup or fail-safe components. The Metrc System infrastructure components are redundant by design to ensure a highly available system.

DISTRIBUTED NETWORK

A distributed network is designed to be resilient and fault tolerant. Metrc guarantees 99.99% network uptime. This is strengthened by our network service provider Cloudflare, which employs Anycast routing to ensure web users are automatically routed around any failures. The combination of this architecture and network produces a reliable, high-performance service. Additionally, geographically separate data centers allow network services to continue operations from an adverse event.

NETWORK SECURITY

Network security begins with integrated security services such as distributed denial-of-service (DDOS) attack protection, Web Application Firewall (WAF), and TLS 1.2 encryption enforcement. Additionally, Metrc utilizes a managed security solution that continuously monitors our infrastructure for signs of intrusion.

DATACENTERS

The Metrc System is hosted in a cloud computing service provided by Azure. Metrc guarantees 99.97% service uptime via our hosting agreement with Azure. Metrc personnel configure and maintain the infrastructure.

These geographically dispersed datacenters comply with key industry standards, such as ISO 27001 and NIST SP 800-53, for security and reliability.

The datacenters are managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world’s largest online services with 24 x 7 continuity. The heart of the Production datacenter site consists of Virtual Machines (VMs). There are three core types of VMs: Domain Controls, Web servers, and Azure SQL databases. Each customer instance of Metrc runs on a highly available set of Web servers and geo-redundant Database servers. The number of VMs can be scaled based on performance needs.

CROSS-REGION DATACENTER REPLICATION

To ensure customers are supported across the world, Azure maintains multiple geographies. These discrete demarcations define a disaster recovery and data residency boundary across one or multiple Azure regions. Cross-region replication is one of several important pillars in the Azure business continuity and disaster recovery strategy. Cross-region replication builds on the synchronous replication of your applications and data that exists by using availability zones within your primary Azure region for high availability. Cross-region replication asynchronously replicates data across other Azure regions for disaster recovery protection.

DATABASE REPLICATION

Azure SQL Database is a fully managed relational database instance with built-in regional high availability and turnkey geo-replication. It provides broad compatibility with SQL Server, enabling on-premises application modernization at scale. It includes intelligence to support self-driving features such as performance tuning, threat monitoring, and vulnerability assessments and provides fully automated patching and updating of the code base. Active geo-replication uses the Always On technology of SQL Server. It asynchronously replicates committed transactions on the primary database to a secondary database by using snapshot isolation.

HIGH AVAILABILITY DESIGN

The Metrc System architecture is a resilient design that does not require the entire system to be brought down for most hardware changes, software updates, or operating system patching and upgrades. Metrc accomplishes this advanced design by incorporating key architectural concepts which include load balancing, redundancy, failover/failback, and virtualization. The strategy is to eliminate any single point of failure through redundant datacenters, network infrastructure, load balancers, firewalls, power delivery.

LOAD BALANCING

Load balancing is a technique to distribute network or application traffic across multiple servers and is used to increase capacity and reliability of applications. A robust load balancing implementation contributes to the reduction of resource contention that impact system availability. Web servers are implemented behind load balancers, so each server is actively processing requests, and will immediately take on the workload of an offline web server Network load balancers are also used to switch to a redundant or standby system upon the failure or unplanned termination of an application, server, system, or network that was previously operating normally. This means that in case of any Metrc system failure, failover does not require human intervention.

Concurrently, the monitoring system notifies the designated personnel about the failure.

BACKUPS

Backups are encrypted and stored in their respective data centers. All backups are stored offsite for at least two weeks. Backups are periodically restored to verify that backups work, and to practice restoration procedures.

FAILOVER/FAILBACK

In the unlikely event that a Metrc system component does fail, Metrc's redundant systems automatically failover to handle the event. During a failover, notifications are sent to all authorized designated personnel. Once the problem is detected and corrected, failback will be performed. Failback is the process of restoring a system, component, or service that is in a status of failover back to the state it was originally in before failure. For example, once we confirm that the production server is operating normally, processing will be switched back to the production server and the backup server will again become the secondary server.

BUSINESS CONTINUITY

Every disaster has one or more causes and effects. Metrc utilizes a planning process influenced by industry standards such as NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems) and ISO 22301:2012 (Business Continuity Management Systems). An important aspect of our approach to disaster recovery and business continuity is to address the critical processes that need to be maintained or restored during the event.

All the following business units have business function continuity even in the event of a disaster impacting our production data center or corporate office:

PRODUCT MANAGEMENT

Product Management consists of a team that focuses on successfully executing a product's lifecycle, from developing new ideas for a product and feature development to working with engineering and design teams to execute the product, all while ensuring that the product will meet the needs of its targeted consumer.

TECHNOLOGY

Metrc's technical and software design as well as operations management practices are critical components that support Metrc's disaster recovery approach and capabilities. Technology is comprised of areas of responsibility such as infrastructure, networking, system administration, software systems development and application support.

INFORMATION SECURITY

Information security personnel support the Metrc System indirectly by monitoring internal and external security threats, administration of antivirus software, maintenance of the inventory of Technology assets, information system security training, and handling compliance related corporate initiatives.

PROVISIONING

Provisioning personnel are primarily accountable for the production, quality assurance, and timely delivery of unique plant and package identifiers (UID) that are used to support Metrc track-and-trace services. The Provisioning operation is currently located in the State of Florida and could be replicated in any required location. We have established procedures so UID provisioning can take place in the event of a disaster. The tag provisioning system is cloud-based and can be accessed from anywhere via an internet connection.

For tags produced, Metrc has contingency procedures to ship the printers to another closely located facility. If moving to the alternative Florida location is determined not to be feasible due to an extensive disaster, then the process calls for spare printers and materials located at our Tennessee facility to be used. These spare printers and materials can be used to provide a reduced output volume during the time immediately following the disaster.

We have agreements in place with multiple suppliers of both printers and raw materials to be able to acquire and take delivery of these resources at the backup provisioning site within days of a disaster.

SUPPORT

Metrc Support personnel are provided as a geographically diverse workforce. The ticketing system is a cloud- based system backed by service level agreement (SLA) agreements. The phone system used for the Help Desk is a cloud-based voice over internet protocol (VoIP) system with SLA backing. For a support agent to be effective, only a computer with an internet connection is required. Additionally, Help Desk employees are geographically separated. For example, our support staff is located in geographically distinct locations such as: Colorado, Florida, Georgia, Tennessee, and Idaho. This allows call routing to areas unaffected by a disaster.

ADDITIONAL BUSINESS UNITS

The Metrc System supporting functions can be provided by employees from remote locations. For example, if a hurricane or earthquake occurs, our employees will use a VPN connection to our corporate network to complete their required tasks from home or another location.

- Program Management has internal interaction with key management, support, development, promote growth, awareness, and name recognition of the Metrc System within strategic accounts, departments, and key influencers
- IT is primarily responsible for provisioning/decommissioning and supporting information systems for Metrc personnel and contractors in accordance with Metrc policies and procedures.
- Finance is responsible for directing the organization's financial planning and accounting, as well as its relationship with financial institutions, insurance companies, accounting and legal firms, payroll service firm, and shareholders.
- People and Culture performs human resources primarily administers employee health and welfare plans and acts as liaison between employees and insurance providers. These personnel resolve benefits-related problems and ensure effective use of plans and positive employee relations. Additionally, they ensure plans are administered in accordance with federal and state regulations and that plan provisions are followed.
- EABD (External Affairs and Business Development) creates documentation and materials to ensure external understanding of the Metrc System via the creation of user guides, integration guides, Request for Proposals (RFP), in- platform instructions, installation/configuration instructions and system operations
- Project Management administers the company's project management software, to include managing projects, updating documentation, identifying training needs and routine upkeep of process templates

METRC SYSTEM SLA

RECOVERY TIME OBJECTIVE

Recovery Time Objectives (RTO) are outlined in our Metrc System Standard Service Level Agreements document.

RECOVERY POINT OBJECTIVE

Recovery Point Objectives (RPO) are outlined in our Metrc System Standard Service Level Agreements document.

ROLES AND RESPONSIBILITIES

The Emergency Response Team will need to assess damage and perform triage on the impact on the disaster. The emergency response team will coordinate with broader executive management, support staff, and program managers to handle disaster recovery related external communications. (ex. state and industry

notifications). Communicate nature of impact and limited access during Recovery and Reconstitution stages of Disaster Recovery Lifecycle. Provide timely updates on impact, changes, and timeline for progress through Disaster Recovery Lifecycle.

EMERGENCY RESPONSE TEAM

ROLE	RESPONSIBILITIES
Technology	Relevant system administrators perform all phases of the Disaster Recovery Life Cycle.
Information Security	Primary architect of Disaster Recovery Life Cycle Stages. Coordinates all aspects of Disaster Recovery testing.
Executive Management	Informed of detection, communication, and status as progressing through the Disaster Recovery Life Cycle stages.
Program Management	Handles written communication of stages as outlined in Disaster Recovery Notification to relevant external entities.

LESSONS LEARNED

After the Disaster Recovery Life Cycle has arrived at the Resumption of Normal Operations, the organization should hold a Lessons Learned meeting to review the effectiveness of the process and identify necessary improvements to existing policy and procedures. The information accumulated from all Lessons Learned meetings should be used to identify and correct systemic weaknesses and deficiencies in policies and procedures. Lessons learned analysis consists of addressing the following questions:

- How well did the staff and management perform?
- Were documented policy and procedures followed?
- Were the procedures adequate?
- Were commitments such as the Metrc System SLA Recovery Time Objective and Recovery Point Objective achieved?
- Were any steps taken that might have inhibited recovery?
- How could information sharing have been improved?
- What tools, processes, metrics or resources could be in place and monitored to address future disasters?
- What could personnel do differently to improve this process?

DISASTER RECOVERY TESTING

Forms of DR testing:

TABLETOP EXERCISE - Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing DR process and individual state of preparedness.

FUNCTIONAL EXERCISE - Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery.

FULL-SCALE FUNCTIONAL EXERCISE - Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility.

POLICY MANAGEMENT

Policies are to be reviewed annually and revised if needed. Policy revisions should be approved in writing by the CTO. Revisions are tracked in the revision and approval History below. Pertinent changes should be communicated to the affected staff members within a reasonable time of the revision release.

PERIODIC REVIEW OF POLICIES

A review of Metrc policies shall be performed on an annual basis. The review will consider policy accuracy, effectiveness, implementation, and compliance. Recommendations resulting from the review will be considered for implementation by executive management.

RECORDKEEPING REQUIREMENTS

Metrc shall maintain the following Records documenting the implementation of this Program:

- This Program and any amendments hereto.
- Reports summarizing any unauthorized access to or unauthorized use of PII, copies of any related notices to Metrc customers or personnel, copies of related notices delivered to federal or state regulatory agencies or other entities, and evidence of mailing of all notices relating to any unauthorized access to or unauthorized use of PII.

REVISION HISTORY

VERSION	CHANGE SUMMARY	APPROVER	TITLE	DATE
2.03	Updated Infrastructure diagram. Lessons Learned documentation incorporated into policy. Formatting changes.	Sam Peterson	CTO	4/13/23
2.02	Separated Azure and Rackspace into distinct documents. Incorporated lessons learned in DR testing exercise.	Zahid Ali	CTO	3/11/22
2.01	Incorporated newest Metrc Brand Guidelines. New language to support new infrastructure, compliance requirements, and version numbering system.	Zahid Ali	CTO	2/14/22
1.05	Reviewed and approved	Zahid Ali	CTO	1/12/22
1.04	Added specific Ransomware Incident Mitigation language	Jesse Naranjo	CTO	1/14/21
1.03	New format and updated content	Jesse Naranjo	CTO	7/15/20
1.02	Updated content	Scott Denholm	Executive Director	12/1/15
1.01	Initial version	Scott Denholm	Executive Director	11/1/15

SCHEDULE G – TRANSITION IN AND OUT

Metrc Data Conversion Plan

Introduction

The primary objective of data conversion is to accurately move work in progress from the source system into the Metrc System to minimize disruption to commerce and regulatory oversight while ensuring data quality. In addition, a successful data conversion retains reporting access to seed-to-sale data, current and historical, and consolidates data sources to reduce the number of data stores the agency is required to work with.

Contractor has designed an approach to converting the agency's data that meets those objectives. The effort will focus on converting data from the legacy seed-to-sale system, but we understand that other smaller systems may also be in scope. Regardless of the source system, we plan the work then perform the work following an iterative process. Each iteration consists of four stages: Data Mapping, ETL (Extract, Transform, and Load), Cleansing, and Validation. The following describes each stage of our Data Conversion Plan as well as indicating when agency participation is involved.

1. Planning

Identifying Agency Participants

One of the first things we work on with the agency is identifying the agency staff who will participate in planning activities including Data Requirements and Source Data Research. Those resources (Agency Data Conversion Team) will identify what data will be converted from the legacy seed-to-sale system and any auxiliary systems in collaboration with Metrc's Data Conversion team. (Agency Data Conversion Team and Metrc's Data Conversion team are referred to collectively as the Joint Data Conversion Team or Joint Team).

The data mapping activity involves engaging your business experts for a series of data-mapping sessions. Ideally, the effort will involve people from a variety of subject areas. The sessions are split up by System function (i.e., plants/harvests, packages, sales, etc.) which allows the agency to assign different personnel to different sessions if desired. Additionally, the agency identifies an Agency Data Conversion Lead who attends all the sessions, at least for the first iteration, in order to maintain continuity across them. The Agency Data Conversion Team also participates in the Validation sessions during which they perform Quality Control on the converted data.

Gathering Data Requirements

Once we have identified participants, we gather data requirements. We identify what data needs to be converted into the Metrc System from the legacy seed-to-sale system. We may determine that all of the legacy data must go into the Metrc System. On the other hand, the legacy seed- to-sale system may include data that is not necessary for oversight of [STATE]'s cannabis regulations, and that data may be determined to be out of scope for conversion. The out-of- scope data could be a candidate for conversion to a legacy reporting database.

We also consider whether data may be conditionally converted based on row-level factors. For instance, we may determine that moving historical data from the legacy seed-to-sale system is not feasible due to historical changes that occurred over time or because it would require extensive data cleanup that cannot be supported. This data would be another candidate for conversion to a legacy reporting database.

In addition to the legacy seed-to-sale system, the agency likely has other, smaller systems that store data related to seed-to-sale tracking. The Joint Data Conversion team will identify those candidate sources and assess whether it makes sense to convert that data into the Metrc System.

If all of the data in the legacy seed-to-sale system is not needed for the Metrc System, then one option is to move that data from the legacy seed-to-sale system into a legacy reporting database from which reports can be run after the transition to the Metrc System.

Researching Source Data

The source data resource process involves gathering information about the source systems, including where the data resides and what documentation is available for them. Having identified the data requirements, we then gather information about both the legacy seed-to-sale system and any other in-scope data sources. That includes understanding the systems that hold the data, the data format, and any data model information or system documentation the agency can provide, especially comprehensive documentation pertaining to the legacy seed-to-sale system.

Information about how source systems are used is almost as important as the system and data architecture documentation. For instance, over the years, the agency may have provided industry and agency users with guidance about how to enter certain data or handle particular situations with respect to the legacy seed-to-sale system. The guidance may have been formal or informal, but either way if it drives the way data is entered, it is a critical input for the Joint Data Conversion team.

Identifying Security Requirements

The Joint Data Conversion Team identifies security requirements around the data stored in the legacy seed-to-sale system. That includes determining whether data is protected using administrative controls, physical security, logical controls, organization standards, and other safeguarding techniques that limit access to unauthorized or malicious users or processes.

Understanding agency requirements and techniques enables the Joint Team to put controls in place to safeguard the agency’s data during the conversion process.

Creating the Project Plan

The Project Plan provides detailed tasks and timelines that are interdependent with other workstreams such as configuration and testing. For instance, if the Metrc System configuration changes and a new data element must be incorporated into the design, the Joint Data Conversion Team must identify the source of that data and convert it into the new system.

Likewise, the user acceptance testing workstream will be incomplete if it does not have sufficient and accurate data to test in the new system. Such interdependencies amongst the workstreams require the Joint Team to build an integrated Project Plan.

Additionally, data conversion activities often carry with them significant risks around legacy data. The risks are somewhat mitigated by the short history of the legacy seed-to-sale system; however, risks may include a lack of a specific data field in the legacy seed-to-sale system that is necessary to populate a required Metrc System data element. As the Joint Data Conversion Team conducts its analysis on the legacy data, it will identify risks and create mitigation plans.

The Project Schedule included in section X of the proposal specifies two full iterations of ETL and validation. In addition, the schedule calls for starting our conversion work early enough that, if risks materialize or any other issues exist after the second iteration, there is time to add a third without impacting the go-live date.

2. Data Mapping

Reviewing Baseline System

A key success factor in data conversion efforts is thinking beyond tables and fields. It is important that the Agency Data Conversion Team understands the target system as a whole, so they have a conceptual understanding of how the data will be used. For that reason, before data mapping begins, we train the Agency Data Conversion Team in use of the Metrc System. The approach will pay dividends during the Data Mapping and Validation stages.

Data Mapping Working Sessions

Data mapping is the bedrock of a successful conversion effort. Once the Joint Data Conversion Team has the legacy data fields identified, it can start the process of identifying the related Metrc System data fields. The Metrc Data Conversion team will define transformation rules that map the elements from the legacy data into the corresponding Metrc System field. We also review the mappings with their agency counterparts and validate the cross references.

Some possible mapping rules are as follows:

- Straight copy – If the source and Metrc System data elements are of the same data type and the column means the same thing in the source system as in the Metrc System, we can just copy the data over.
- Simple translation – A straightforward mapping from one set of values to another. For instance, we may map existing reason codes in the legacy seed-to-sale system to Metrc System action reasons.
- Complex translation – Some mappings will require using multiple tables or fields in the source to determine what gets stored in a Metrc System row or data element.
- Generation – There may be situations where there is no suitable data in the source system to map to a required column. In such cases, the group can identify how it should be populated. For instance, if the agency's legacy seed-to-sale system does not assign manifest numbers (admittedly an unlikely example), the group may decide to assign sequential numbers to existing transfers.

One important factor in the effort is to limit the use of default rules (e.g., “plants that meet criteria x should convert as immature, plants that meet criteria y are flowering, and all others are vegetative”). It is better practice to specifically identify the criteria for vegetative plants: “plants that meet criteria x should convert as immature, plants that meet criteria y are flowering, plants that meet criteria z are vegetative, and all others should flag a conversion error.” This gives us the opportunity, later in the ETL and Data Cleansing stages, to identify data conditions we did not originally contemplate and address them in the next iteration.

The outcome of these sessions is a series of mappings to Metrc System tables and fields. We focus on fields that are required by the Metrc System first, then the desired ones.

Exceptions

Data mapping then looks at data in the source systems for which there is no defined mapping to the Metrc System. It is certainly possible that some sources may contain data that does not fit into the Metrc System. If that is the case for the majority of data elements from a particular system, we might reassess whether that source system is in scope for the seed-to-sale data conversion effort or should be retired. Alternatively, we may define an extract process without any transformation into a reporting database. Similarly, any row-level data from the legacy seed- to-sale system that the group opts not to convert to the Metrc System will be stored in such a database.

System Configuration Updates

As discussed below, the Joint Team monitors ongoing configuration discussions, so we can consider any potential changes after the baseline configuration. For instance, if the Development and Prototyping phase of the implementation process results in a decision to add a new transfer type, we will revisit transfer type mappings to determine if and how they should change. This allows us to make progress on data conversion while minimizing the impact of changes that will affect that work.

3. Extract, Transform, and Load

With the initial data mapping complete, the Metrc team creates ETL (extract, transform, and load) scripts that move data from the source systems into the Metrc System. We may use test data from the source systems to test the scripts, but once coding is complete, we run the ETL against the production source systems to create Metrc System data in a testing instance. This data will be used for the Validation process.

The ETL stage includes four steps, described below:

- Extracting data from legacy system
- Transforming data
- Loading data into the Metrc System
- Testing data load

We determine the appropriate ETL tool during the Planning stage, as we discover the structure and content of the legacy database. The tool selected may be based on the number of records, the complexity of the mappings, and the degree to which transformation and cleansing may be required. The Metrc team has experience using the

Azure Data Factory and has developed custom programs using SSIS from SQL server and various Python scripts with SQL.

Extracting Data

The Joint Data Conversion Team and the owners of the legacy systems extract data from the legacy system according to the data mappings templates. Typically, this means that data is sent from the legacy seed-to-sale system to a new format in an intermediate staging area where the data can be readily viewed and cleansed as needed. The extraction process is either conducted manually or a program is written to automate the process. The approach taken depends on the number and complexity of the fields and records involved.

Transforming Data

The Joint Team starts developing transformation rules during the Data Mapping stage. We implement those transformation rules—such as straight copy, simple or complex translation— during the ETL stage, writing code to transform data from the legacy structure to the Metrc System structure. That ensures not only that the data is moved into the appropriate Metrc System field but also that the Metrc System picks up where the legacy system left off.

Loading Data

Once the data is transformed, it can be loaded into the Metrc System by the ETL tool or program. If more than one mapping template was developed, then the Joint Data Conversion Team sequences the loading to ensure that fundamental data elements are present in the system and can then be associated to new templates as they are loaded. (If this is the case, then keys are built into the templates so their records can be associated with one another.)

ETL Testing

The loading is conducted through an automated process. Before loading of actual data takes place, the Joint Team tests the load process to ensure that it properly puts the right data into the correct fields and that it produces the right number of records.

At this point, we also run reports that measure how clean the data is based on criteria defined during the Data Mapping stage. An example of such a metric is what percentage of the plant records in the source data pass all of the validations we have defined. In addition to defining the metric, we set target thresholds beforehand—such as “99.5% of plant data was converted and met our validation rules.” That allows us to assess our progress and identify any risks or issues.

4. Data Cleansing

Data cleansing is the process of identifying inaccurate, incomplete, or irrelevant records from the legacy systems and correcting or eliminating data fields to make the source data consistent with Metrc System requirements. Data cleansing involves analyzing the legacy applications for data correctness, completeness, and convertibility. Its aim is to support data quality by eliminating the following data inconsistencies:

- Duplicate data
- Non-standardized data
- Obsolete or inactive records

- Compound and incomplete data fields

Although data cleansing is identified here as occurring later in the iterative cycle, it may actually start quite early in the overall data conversion process. For instance, if there are known issues in the source data, the Joint Data Conversion Team may start addressing them as soon as they are discovered. Alternatively, the agency may recognize issues with data quality based on its use and experience with the system. The team develops a plan to undertake cleansing, whether it be achieved by manual process or, if possible, through the ETL tool or process identified during the Planning stage.

5. Data Validation

The purpose of data validation is to determine whether data from the legacy systems is appropriately represented in the Metrc System. The Metrc team will guide this effort and offer insight into how the Metrc System will work with the data as converted. While to some extent this could be viewed as a field-by-field comparison, the real test of success or failure is whether the data is converted such that the Metrc System will report and process it as expected.

As an output of the ETL process, the Metrc Data Conversion team generates reports that support validation (helping the team assess what data is ready to be validated and providing a comparison of key counts like the number of packages in the Metrc System as compared to the legacy system).

The Agency Data Conversion Team members will look at data in the legacy seed-to-sale system side-by-side with the Metrc System to get a holistic understanding of whether a facility and all of their plants and packages converted correctly. They may run reports within the Metrc System, attempt to initiate transfers, etc., to make sure that the data not only is converted and looks correct but also behaves as expected in the Metrc System.

If it turns out that some data did not translate correctly to how it will be used in the Metrc System, Metrc's Data Conversion team will first confirm whether the ETL process accurately reflected the decisions made during the Data Mapping stage. If not, we will determine with the Agency Data Conversion Team whether the issue merits an immediate fix and rerun, or whether the fix should be implemented in a later iteration.

If the ETL process correctly implemented the mapping decisions but the data is still incorrect, there are a few options for proceeding:

- If the problem is that the data in the source system does not conform to expected inputs, we can run a report of that data condition for cleansing in the legacy system.
- If the data and mapping are correct, but the data needs to be transformed differently, we can modify the transformation rules.
- If the mapping is incorrect, we can modify it as appropriate (change the rules, handle more different situations, etc.).
- For low-volume changes for which it would be complex or impossible to create transformation rules, identify workarounds for manually moving the data after automated conversion is complete. For instance, if a small number of plants have corrupted data due to a bug in the source system, the agency may opt for manual entry. In that case, we would generate a list of those plants and provide the agency or licensees procedures for entering them into the Metrc System.

In this way, the output from the validation feeds directly into the next iteration.

Go-Live and Post Implementation Validation

When the go-live date has been established, the Joint Data Conversion Team will establish a blackout period during which no data is entered into the legacy seed-to-sale system while the system cutover takes place. This may be different for each of the different modules and may depend upon the volume of transactions involved. The cutover plan will include the timing and sequence of the data load.

The agency and Metrc may determine that it is necessary to monitor transactions in both systems to ensure that the Metrc System is performing as expected and it is producing the business outcomes intended by the design. A key part of this evaluation will be looking at the data and transaction results in the new system and comparing it to the data in the legacy system.

SCHEDULE H – HARDWARE

The State currently has seven RFID Handheld units, two are owned and five are under lease. Contractor will transfer ownership of the five under lease to the CRA as part of a contract under this contract, which will bring the total units in CRA's possession to fourteen.

Contractor agrees to Schedule H - Hardware

1. **Definitions**. All initial capitalized terms in this Schedule that are not defined herein shall have the respective meanings given to them in the Contract.

2. **Hardware**. Contractor must provide fully functioning Hardware that fully integrates with the Software and performs in accordance with the requirements and specifications set forth in the Contract.

3. **Delivery**. Contractor must deliver the Hardware to the locations designated by the State by the delivery date specified in the Statement of Work, or as otherwise specified in writing by the State. Five (5) Business Days prior to the actual delivery date, Contractor must give written notice to the State specifying the precise delivery date and time. Contractor must pay all costs associated with replacing any item damaged in transit to the final destination. Contractor acknowledges that no item will be considered delivered on the delivery date if it is damaged or otherwise not ready for the State to begin its acceptance procedures. Contractor must, at a minimum, package the Hardware according to industry standards and include a packing slip with each shipment. Contractor must also arrange for any rigging and drayage necessary to deliver the Hardware. All costs associated with packaging, shipping, transportation, delivery and insurance are to be borne by Contractor.

4. **Installation, Integration and Configuration.**
   a. Contractor must unpack, assemble, install, integrate, interconnect, configure and otherwise provide and make fully operational all the Hardware at the locations specified by the State prior to the applicable dates in accordance with the criteria set forth by the State. Where necessary to complete installation, Contractor must provide all required moving and installation resources, including but not limited to personnel, packing material, and floor protection panels as necessary. After completing installation, Contractor must

provide the State with written notification that the Hardware is ready for use and acceptance.

b. Contractor must supply all materials required to complete the assembly, installation, integration, interconnection, and configuration of the Hardware at the locations specified by the State so that it is ready for use and acceptance, including providing and setting up all required connections to the power supply and any other necessary cables and any other accessories or supplies.

c. Contractor must leave all work areas clean once installation is complete, which includes removing and disposing of all packing materials.

d. Unless otherwise provided for in the Pricing Schedule, all costs associated with the installation services described in this Section are to be borne by Contractor.

5. **Documentation**. Contractor must provide to the State all end-user documentation for the Hardware. The documentation, at a minimum, must include all the documentation available to consumers from the manufacturer of the Hardware about the technical specifications of the Hardware, installation requirements, and operating instructions, as well as details about the software programs with which the Hardware functions.

6. **Acceptance**. This Section applies to the acceptance of the Hardware itself. Acceptance of the Hardware may be conditioned on System Acceptance in Schedule I.

a. The Hardware is subject to inspection and acceptance by the State. As part of its acceptance process, the State may test any function of the Hardware to determine whether it meets the requirements set forth in this Contract. If the State accepts the Hardware, the State will notify Contractor in writing. Unless otherwise provided in the Statement of Work, if the Hardware is not fully accepted by the State, the State will notify Contractor in writing that either: (a) the Hardware is accepted but noted deficiencies must be corrected; or (b) the Hardware is rejected. If the State finds material deficiencies, it may: (i) reject the Hardware without performing any further inspections; (ii) demand performance at no additional cost; or (iii) deem such material deficiencies to be a breach of the Contractor's obligations under the terms of the Contract and terminate this Contract in accordance with Section 16.

b. Within 10 Business Days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Hardware, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Hardware to the State. If acceptance with deficiencies or rejection of the Hardware impacts the content or delivery of 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.

c. If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may provide the Hardware and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

d. Acceptance by the State does not relieve Contractor of its responsibility for defects in the Hardware or other failures to meet the requirements of the Contract or of its support and maintenance obligations.

7. **Support and Warranty for Hardware**.

a. Throughout the Term, Contractor will provide maintenance and support of the Hardware and will repair, service, or replace any defective or nonconforming Hardware in accordance with the requirements set forth in this Contract, including without limitation the Service Level Agreement.

b. Contractor will provide and assign or otherwise transfer to the State or its designee all manufacturer's warranties regarding all Hardware or as otherwise provided for in the Contract.

8. **Further Representations and Warranties.** Contractor represents and warrants that:

a. all Hardware is delivered free from any security interest, lien, or encumbrance and will continue in that respect;

b. the Hardware will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party;

c. it has and will retain the unconditional and irrevocable right, power and authority to provide to the State the Hardware throughout the Term and any additional periods during which Contractor does or is required to provide Hardware to the State; and

d. all hardware includes the manufacturing warranty.

9. **Risk of Loss and Title**. Until final Acceptance, title and risk of loss or damage to Hardware remains with Contractor. Contractor is responsible for filing, processing, and collecting all damage claims. The State will record and report to Contractor any evidence of visible damage. If the State rejects the Hardware, Contractor must remove the Hardware from the premises within 10 calendar

days after notification of rejection. The risk of loss of rejected or nonconforming Hardware remains with Contractor. Rejected Hardware not removed by Contractor within 10 calendar days will be deemed abandoned by Contractor, and the State will have the right to dispose of it as its own property. Contractor must reimburse the State for costs and expenses incurred in storing or effecting removal or disposition of rejected Hardware. Title passes to the State upon final Acceptance of the Hardware.

SCHEDULE I – SYSTEM ACCEPTANCE

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

"**System**" has the meaning set forth in Subsection 2.1(a) of this Schedule.

"**System Acceptance**" has the meaning set forth in Subsection 2.6 of this Schedule.

"**System Acceptance Tests**" means such tests as may be conducted in accordance with this **Schedule** to determine whether the System meets the requirements of this Contract.

"System Integration Testing" has the meaning set forth in Subsection 2.2(a) of this Schedule.

"System Testing Period" has the meaning set forth in Subsection 2.1(b) of this Schedule.

2. System Acceptance Testing.

2.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software and Hardware together (the "**System**"), or upon any changes to such System, System Acceptance Tests will be conducted as set forth in this **Schedule** to ensure the System as a whole conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All System 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 the receipt by the State of written notification that the System is ready to have System Acceptance Tests performed, 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 "**System Testing Period**"). System 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 System Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such System Acceptance Tests; and

(ii) for System Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such System Acceptance Tests.

2.2 Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of System Acceptance Tests.

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

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

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

(a) If such notice is provided by either party and identifies any Nonconformities, the parties' rights, remedies, and obligations will be as set forth in **Subsections 2.4** and **2.5**.

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

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

(i) notify Contractor in writing of Nonconformities the State has observed in the System and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Subsections 2.4** and **2.5**; or

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

2.4 Failure of Acceptance Tests. If System Acceptance Tests identify any Nonconformities, Contractor, at Contractor's sole cost and expense, will remedy all such Nonconformities and re-deliver the System, or relevant portion thereof, 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 System Acceptance Tests, in the case of System Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Subsections 2.3(a)** or **2.3(c)(i)**, identifying any Nonconformities.

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

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

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

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

2.6 System Acceptance. Acceptance of the System ("**System Acceptance**") (subject, where applicable, to the State's right to System Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the System under **Subsection 2.3(b)**, or **2.3(c)(ii)**

STATE OF MICHIGAN
PROCUREMENT
Michigan.gov/MiProcurement