STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES

Department of Technology, Management, and Budget
320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**
to
Contract Number **230000000198**

CONTRACTOR	Amazon Web Services, Inc.
	410 Terry Avenue North
	Seattle, WA 98109-5210
	Eric Hill
	248-224-9051
	echill@amazon.com
	VS0160030

STATE	Program Manager	Jason Frost	DTMB
		517-636-6505	
		frostJ@Michigan.gov	
	Contract Administrator	Matt Weiss	DTMB
		(517) 256-9895	
		weissm4@michigan.gov	

CONTRACT SUMMARY

STATE INTEGRATED IAAS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
December 6, 2022	December 6, 2027	5 - 1 Year	December 6, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		N/A

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$100,000.00	$1,050,830.00	$1,150,830.00

DESCRIPTION

Effective 1/26/2024, this Contract is hereby increased by $1,050,830.00. MDHHS previously purchased AWS Services from an authorized AWS reseller in the AWS Partner Network to support programs such as MiResident Outreach and MiBridges. The State will now purchase these Services directly from AWS. $985,000 is added for these Services. This projected amount is estimated to cover the period 1/1/24-9/30/24. $65,830.00 is added for AWS training sessions and materials on the AWS Skill Builder Learning Portal.

The State is responsible for all applicable fees and charges accrued for use of the Service Offerings regardless of the value identified herein.

All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, DTMB procurement and State Administrative Board approval on 12/6/2022.

DESCRIPTION OF SERVICES -
IT CHANGE NOTICE

Project Title: MCP AWS Skill Builder Training Subscription	**Period of Coverage:** 1/1/2024 – 12/31/2024
Requesting Department: DTMB	**Date**: 12/15/2023
Agency Project Manager: Nicole Raynak	**Phone**: (517) 763-7034
DTMB Project Manager: David Tremblay	**Phone**: (517) 256-9364

BACKGROUND:

Department of Technology, Management and Budget (DTMB) – Platform, Design and Support Services (PDSS) is onboarding the Michigan Cloud Provider program. Once fully onboarded, this program will allow PDSS to facilitate State of Michigan (SOM) agencies use of the Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) public clouds.

Currently, DTMB-PDSS has hired multiple contract resources to assist in this new service offering. However, to successfully transition this service to a Maintenance & Operations model, DTMB-PDSS full-time employees (FTE) must be able to effectively support and provide this service. The transition of skills and knowledge requires the FTE to be trained in and familiar with the external clouds. Therefore, learning subscriptions are required.

PROJECT OBJECTIVE:

This document describes the purchase of access to AWS Learning portal for AWS-specific training. Effective implementation of the AWS cloud is not feasible without training for FTEs supporting the Amazon cloud service.

DESCRIPTION OF SERVICES

This Description of Services describes the purchase of AWS training sessions and materials on the AWS Skill Builder Learning Portal.

The purchase of the AWS Skill Builder Team Subscription is subject to Contract #230000000198 (the “Agreement”); and is subject to the AWS Training Policies in effect as of the date AWS receives email response confirming the details of the order below (the “Effective Date”), available at https://aws.amazon.com/training/aws-training-policies/, which details the fees and other terms relevant to the AWS Skill Builder Team Subscription. Notwithstanding Section 2.3 of the AWS Training Policies, access to Team Subscription will commence on the Preferred Start Date stated below.

The Team Subscription is a paid year-long AWS Training Service Offering through which customers purchase subscriptions for a certain number of Learners to access premium AWS-built Training content (“Seats”). This is in addition to the free content on AWS Skill Builder. You assign Seats to employees and contractors (“Learners”). You also have administrative capabilities, such as assigning training to Students, enabling single sign-on (SSO) access, and creating training progress reports.

PAYMENT:

V4-082023	
Customer name This name will be visible in the administrator environment.	State of Michigan/DTMB
Learning Administrators Learning Administrators will be able to manage Learners, course enrollments, and view reports.	Name(s): Mary McGinnis Email(s): mcginnism2@michigan.gov
Allowed email domains If requested AWS will restrict the email domains Learners can use to sign in. Please provide the email domains that will be used by your employees if applicable. We don't need the list of all Learner emails, only the email domains, i.e.; @amazon.com.	@michigan.gov
Billable Account ID Specify which single account to bill the AWS Skill Builder Team Subscription fees.	281149291541
Billing Term Note: Only Annual Billing is offered for the Skill Builder Team Subscription	Annual Billing
Preferred Start Date Specify the date you would like to access your Seats. You can select any business day except a date that falls within the last 2 business days of the month. Your Preferred Start Date must be at least 20 days after the date you agree to your Skill Builder purchase.	February 6, 2024
Seats Ordered Specify the number of AWS Skill Builder Team Subscription Seats ordered in this transaction.	170
Price This is the total amount that will be charged to the Billable Account ID you identify above. Please note that this amount is exclusive of applicable taxes and duties, including VAT and applicable sales tax.	$65,830
Single Sign-On Is Single Sign-On (SSO) access to the environment desired?	No

Payment will be based upon:

- Invoicing and payment terms are subject to Contract #230000000198 (the "Agreement")

PROJECT CONTACTS:

The designated Agency Project Manager is:

Name: Nicole Raynak
Department: DTMB
Area: Platform, Design & Support Services – Business Operations Support Services
Building/Floor: Operations Center
Address: 7285 Parsons
City/State/Zip: Dimondale, MI 48821
Phone Number: (517) 763-7034
Email Address: Raynakn@michigan.gov

The designated DTMB Project Manager is:

Name: David Tremblay
Department: DTMB
Area: Platform, Design & Support Services – Design Services
Building/Floor: Operations Center
Address: 7285 Parsons
City/State/Zip: Dimondale, MI 48821
Phone Number: 517-256-9364
Email Address: TremblayD1@michigan.gov

AGENCY RESPONSIBILITIES:

DTMB-PDSS is responsible for providing user identification to AWS for successful enrollment in the AWS Skill Builder Learning Portal. Payment shall be in accordance with Contract Number 230000000198 payment terms.

This order is subject to Contract Number 230000000198. All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, DTMB procurement.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **230000000198**

CONTRACTOR	Amazon Web Services, Inc.
	410 Terry Avenue North
	Seattle, WA 98109-5210
	Eric Hill
	248-224-9051
	echill@amazon.com
	VS0160030

STATE	Program Manager	Jason Frost	DTMB
		517-636-6505	
		frostJ@Michigan.gov	
	Contract Administrator	Matt Weiss	DTMB
		(517) 256-9895	
		weissm4@michigan.gov	

CONTRACT SUMMARY

STATE INTEGRATED IAAS

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
December 6, 2022	December 6, 2027	5 - 1 Year	December 6, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		N/A

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$100,000.00	$0.00	$100,000.00

DESCRIPTION

Effective 12/1/2023, a one-time exception will occur opening the Infrastructure as a Service (IaaS) prequal program scope to consolidate current AWS account(s) under a single agreement. This will allow any AWS account(s) made before 12/1/2023 through other purchasing vehicles to be pulled under the existing IaaS contract.

DTMB shall take any actions needed to qualify as an "AWS Enterprise Account" under this Contract. Additionally, AWS shall only be required to pay any required administrative fee under the Contract once such accounts qualify as an "AWS Enterprise Account."

All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, DTMB procurement and State Administrative Board approval on 11/30/2023.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**
to
Contract Number **230000000198**

CONTRACTOR	Amazon Web Services, Inc.
	410 Terry Avenue North
	Seattle, WA 98109-5210
	Eric Hill
	248-224-9051
	echill@amazon.com
	VS0160030

STATE	Program Manager	Jason Frost	DTMB
		517-636-6505	
		frostJ@Michigan.gov	
	Contract Administrator	Matt Weiss	DTMB
		(517) 256-9895	
		weissm4@michigan.gov	

CONTRACT SUMMARY			
STATE INTEGRATED IAAS			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
December 6, 2022	December 6, 2027	5 - 1 Year	December 6, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		N/A

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$0.00	$100,000.00	$100,000.00

DESCRIPTION

Effective 3/7/2023, this Contract is hereby increased by $100,000 to allow DTMB - CTO to launch management services in the AWS cloud.

The State is responsible for all applicable fees and charges accrued for use of the Service Offerings regardless of the value identified herein.

All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency and DTMB procurement.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES

Department of Technology, Management, and Budget

320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**

to

Contract Number **230000000198**

CONTRACTOR	Amazon Web Services, Inc.
	410 Terry Avenue North
	Seattle, WA 98109-5210
	Eric Hill
	248-224-9051
	echill@amazon.com
	VS0160030

STATE	Program Manager	Jason Frost	DTMB
		517-636-6505	
		frostJ@Michigan.gov	
	Contract Administrator	Matt Weiss	DTMB
		(517) 256-9895	
		weissm4@michigan.gov	

CONTRACT SUMMARY			
STATE INTEGRATED IAAS			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
December 6, 2022	December 6, 2027	5 - 1 Year	December 6, 2027

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		N/A

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$0.00	$0.00	$0.00

DESCRIPTION

Effective 1/27/2023, the following amendment is hereby incorporated to update Attachment A and add the IRS Publication 1075 Customer Addendum.

All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency and DTMB procurement.

AMENDMENT NO. 1 TO STATE OF MICHIGAN ENTERPRISE AGREEMENT

This Amendment No. 1 (this "**Amendment**") by and among AWS Contracting Parties identified in the signature blocks below, any other AWS Contracting Party that is added to the Agreement pursuant to Section 12.4 of the Agreement (collectively, "**AWS**"), and State of Michigan ("**Customer**") is effective as of December 22, 2022 (the "**Amendment Effective Date**") and is an amendment to the State of Michigan Enterprise Agreement (the "**Agreement**") dated December 6, 2022 by and among Amazon Web Services, Inc. and Customer. Unless otherwise defined in this Amendment, all capitalized terms used in this Amendment will have the meanings ascribed to them in the Agreement. The parties agree as follows:

Amended Terms

1. Attachment A. Attachment A of the Agreement is deleted and replaced with the following:

"Attachment A
AWS Account ID(s):

The list above includes any Master Account or Member Accounts joined to such accounts via AWS Organizations, as described in the Service Terms.

Customer may add AWS accounts to the list above or remove AWS accounts from the list above by providing notice to AWS via email to enterprise-accounts@amazon.com and aws-michigan-ea@amazon.com, that includes (1) Customer's full name, (2) the Enterprise Agreement number (which begins with "CC" and is found on the upper right corner of each page of this Agreement), and (3) the AWS Account ID of each added or removed AWS account. Upon Notice, AWS may replace the notification process or make available another means of adding and removing AWS accounts to the list above."

2. IRS Publication 1075 Customer Addendum. The attached IRS Publication 1075 Customer Addendum is added to this Agreement.

Miscellaneous

3. **Entire Agreement; Conflict.** Except as amended by this Amendment, the Agreement will remain in full force and effect. This Amendment, together with the Agreement as amended by this Amendment: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof. If there is a conflict between the Agreement and this Amendment, the terms of this Amendment will control.

4. **Counterparts and Facsimile Delivery.** This Amendment may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this Amendment by facsimile or email transmission.

(Remainder of Page Intentionally Left Blank)

IN WITNESS WHEREOF, the parties have executed this Amendment as of the Amendment Effective Date.

AMAZON WEB SERVICES, INC.

By: ____
Name: ______________________________________
Title: _______________________________________
Signature Date: ______________________________

STATE OF MICHIGAN

By: ____
Name: ______________________________________
Title: _______________________________________
Signature Date: ______________________________

[*Signature Page to Amendment No. 1 to AWS Enterprise Agreement*]

IRS Publication 1075 Customer Addendum

This IRS 1075 Addendum (this "**Addendum**") is entered into by the AWS Contracting Party[ies] identified in the signature blocks below (collectively "**AWS**") and State of Michigan ("**Customer**") and is effective as of November 8, 2022 (the "**Addendum Effective Date**"). This Addendum supplements the AWS Customer Agreement available at http://aws.amazon.com/agreement, (as updated from time to time) between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Service Offerings (the "**Agreement**"). Unless otherwise defined in this Addendum, all capitalized terms in this Addendum have the meanings set forth in the Agreement. The parties agree as follows.

1. General

1.1 Customer agrees that this Addendum only applies to Customer Content subject to IRS Publication 1075 and Services listed as those that can be configured to meet IRS Publication 1075 requirements at https://aws.amazon.com/compliance/irs-1075/, or its successor site.

1.2 AWS and Customer agrees that IRS Publication 1075 and Exhibit 7 - Safeguarding Contract Language will be satisfied as set forth in this Addendum.

2. Customer Responsibilities

2.1 Customer is solely responsible for ensuring that IRS Publication 1075 requirements are fulfilled prior to introducing Customer Content that includes Federal Tax Information ("FTI"), as defined under IRS Publication 1075, into the Service or Service Offerings. Customer agrees to configure the Services in such a manner that it prevents AWS from having logical access to Customer's FTI.

2.2 Customers have a variety of options to choose from when configuring their accounts for all sensitive or otherwise valuable Content including FTI. AWS recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings as Customer determines is appropriate, in order for Customer to comply with IRS Publication 1075 or other legal or regulatory requirements applicable to Customer.

2.3 Customer understands that AWS Services operate under a shared security model where security and compliance is a shared responsibility between AWS and the customer. Customers are responsible for security in the cloud and must configure the Services as part of its security responsibilities. Customer agrees that its compliance with IRS Publication 1075 is dependent upon on Customer's configuration of the Services and adoption and implementation of policies and practices. Documentation for the Services includes information that may help the Customer comply with IRS Publication 1075 requirements.

3. Customer Inspection Rights

3.1 Provided that the Customer and AWS have a NDA in place, Customer will be provided (i) through AWS Artifact, access to information generated by AWS's regular monitoring of security, privacy, and operational controls in place to afford you an ongoing view into the effectiveness of such controls;

and (ii) upon request, be afforded the opportunity to communicate with AWS's subject matter experts for clarification of the reports identified above.

3.2 Notwithstanding anything to the contrary in Attachment A, Customer will use the information from Section 3.1 herein to satisfy any inspection requirements under IRS Publication 1075. Customer agrees that the audit rights described in this section are the sole rights to be provided in full satisfaction of any audit that may otherwise be requested by the IRS or Customer. Notwithstanding anything to the contrary in Attachment A, AWS will not grant any inspection rights to Customer or access to data centers or other facilities that may cause AWS to be non-compliant with its contractual obligations under FedRAMP, ISO 27001/27018, other US Government security related operations, or its security policies.

3.3 Information provided by AWS is confidential and subject to the NDA. Upon request and pursuant to appropriate confidentiality protections, Customer shall be permitted to provide information described in Section 3.1 to the IRS to satisfy the IRS inspection requirements under IRS Publication 1075.

IN WITNESS WHEREOF, you and AWS have executed this Addendum as of the Addendum

Effective Date.

AMAZON WEB SERVICES, INC.

By: ___________________________________

Name: _________________________________

Title: __________________________________

Date signed: ___________________________

STATE OF MICHIGAN

By: ___________________________________

Name: _________________________________

Title: __________________________________

Date signed: ___________________________

Attachment A

(IRS Publication 1075, Exhibit 7)

I. PERFORMANCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

II. CRIMINAL/CIVIL SANCTIONS

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

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

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

(4) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically,

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

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

III. INSPECTION

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

CC OTH 00723966 2022 TR

STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management, and Budget
Elliott-Larsen Building, 320 S Walnut St #6, Lansing, MI 48933

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **230000000198**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	Amazon Web Services, Inc.
	410 Terry Avenue North
	Seattle, WA 98109-5210
	Eric Hill
	248-224-9051
	echill@amazon.com
	VS0160030

STATE	Program Manager	Jason Frost	DTMB
		517-636-6505	
		frostJ@michigan.gov	
	Contract Administrator	Matt Weiss	DTMB
		517-256-9895	
		weissm4@michigan.gov	

CONTRACT SUMMARY				
DESCRIPTION: State Integrated IaaS				
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**	
December 6, 2022	December 6, 2027	5, 1 year	December 6, 2027	
PAYMENT TERMS		**DELIVERY TIMEFRAME**		
Net 45		NA		
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**	
☐ P-card	☐ Payment Request (PRC)	☐ Other	☒ Yes	☐ No
MINIMUM DELIVERY REQUIREMENTS				
NA				
MISCELLANEOUS INFORMATION				
NA				
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION		**$0.00**		

legal

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

Agency

Date

STATE OF MICHIGAN ENTERPRISE AGREEMENT

This Enterprise Agreement (this “Agreement” or “Contract”) is made and entered into by and among the AWS Contracting Parties specified on this Cover Page, any other AWS Contracting Party that is added to this Agreement pursuant to Section 12.14, and the customer specified on this Cover Page (“Customer” or “State”). The AWS Contracting Parties are collectively referred to herein as “AWS” or “Contractor.”

In consideration of the mutual promises contained in this Agreement, AWS and Customer agree to all terms of the Agreement effective as of December 6, 2022 (the “Effective Date”).

Defined terms used in this Agreement with initial letters capitalized have the meanings given in Section 13 below.

AWS Contracting Party:	**Customer Name:**
Amazon Web Services, Inc.	**Michigan Department of Technology, Management and Budget**
By: ______________________________	**By:** ______________________________
Name: ______________________________	**Name:** ______________________________
Title: ______________________________	**Title:** ______________________________
Signature Date: ____________________	**Signature Date:** ____________________
Address:	**Address:**
410 Terry Avenue North, U.S.A. **Seattle, WA 98109-5210** **Attention: AWS General Counsel** **Fax: 206-266-7010**	**Elliott-Larsen Building, 320 S Walnut St #6,** **Lansing, MI 48933** **Attention: Matt Weiss** **Phone: 517-256-9895** **E-mail: weissm4@michigan.gov**

1. Use of the Service Offerings.

1.1 Generally. Customer may access and use the Service Offerings in accordance with this Contract. Service Level Agreements apply to certain Services. Customer's use of the Service Offerings will comply with the terms of this Contract.

1.2 Contractor Account. To access the Services, Customer must create one or more Contractor Enterprise Accounts. Unless explicitly permitted by the Service Terms, Customer will only create one Contractor Enterprise Account per email address. All Contractor Enterprise Accounts will be covered by this Contract. For all Contractor Enterprise Accounts, this Contract supersedes any acceptance of the AWS Customer Agreement by Customer or any of its employees acting on behalf of Customer. If any of Customer's Contractor accounts do not meet the definition of a "Contractor Enterprise Account," those accounts will be governed by the AWS Customer Agreement.

1.3 Third-Party Content. Third-Party Content may be used by Customer at Customer's election. Third-Party Content is governed by this Contract unless accompanied by separate terms and conditions, which may include separate fees and charges.

1.4 Customer Affiliates. Any Customer Affiliate may use the Service Offerings under its own AWS Enterprise Account(s) under the terms of this Agreement by executing an addendum to this Agreement with AWS, as mutually agreed by AWS and the Customer Affiliate.

1.5 Chain Subcontractors. At least 180 days prior to authorizing a Chain Subcontractor (as defined below), AWS will add that Chain Subcontractor to the list of Chain Subcontractors on AWS's website including the name of the Chain Subcontractor and a description of the services provided (the "**Chain Subcontractor List**"). Notwithstanding the foregoing, with respect to any Chain Subcontractor which provides a portion of the AWS Services that is not generally available as of the Effective Date, AWS will not be required to update the Chain Subcontractor List until the date such portion of the AWS Services is made generally available. A "**Chain Subcontractor**" is a subcontractor to whom AWS has subcontracted a portion of the AWS Services, where the subcontractor's role is such that its failure to perform would have a significant effect on AWS's ability to provide the AWS Services in accordance with AWS's obligations under this Agreement. AWS will (a) enter into a written agreement with the Chain Subcontractor and will impose obligations, as appropriate in light of the Chain Subcontractor's role and duties, such as confidentiality, data protection, data security, business continuity and audit, (b) remain fully responsible under this Agreement for the provision of the portion of AWS Services performed by the Chain Subcontractor, and (c) perform due diligence on the Chain Subcontractor.

2. Changes.

2.1 To the Service Offerings. AWS may change or discontinue any of the Service Offerings, from time to time. For any Contractor Enterprise Accounts enrolled in AWS Support at the Developer-level tier or above (or any successor service providing such communications alerts), AWS will provide at least 12 months prior Notice to Customer if AWS decides to discontinue a Service that it makes generally available to its customers and that Customer is using. AWS will not be obligated to provide Notice under this Section 2.1 if the discontinuation is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity.

2.2 To the Service Level Agreements. AWS may change Service Level Agreements from time to time, but will provide 90 days' prior Notice to Customer before materially reducing the benefits offered to Customer under any Service Level Agreement(s) that are available as of the Effective Date.

3. Privacy and Security.

3.1 Contractor Security. AWS will implement reasonable and appropriate measures for the Contractor Network (as determined by Contractor) designed to help Customer secure Customer Content against accidental or unlawful loss, access or disclosure (the "**Security Objectives**") in accordance with the Contractor Security Standards. AWS may modify the Contractor Security Standards from time to time, but will continue to provide at least the same level of security as is described in the Contractor Security Standards on the Effective Date.

3.2 Data Privacy.

Customer may specify the AWS regions in which Customer Content will be stored. Customer consents to the storage of Customer Content in, and transfer of Customer Content into, the AWS regions Customer selects. AWS will not access or use Customer Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. AWS will not (a) disclose Customer Content to any government or third party, or (b) subject to Section 3.3, move Customer Content from the AWS regions selected by Customer; except in each case as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, AWS will give Customer reasonable Notice of any legal requirement or order referred to in this Section 3.2, to enable Customer to seek a protective order or other appropriate remedy. Where a binding order of a governmental body is based upon a legal requirement of – or is alleged by a governmental entity or court order in – a jurisdiction in which the Customer does not store Customer Content covered by the requirement or allegation (a "Foreign Requirement"), AWS will:

(a) Provide Customer with reasonable prior notice of the Foreign Requirement;
(b) Afford Customer a reasonable opportunity to comply with or otherwise challenge or address the Foreign Requirement; and
(c) Make available appropriate AWS personnel available to discuss possible resolution of the matter.

AWS will only use Account Information in accordance with the Privacy Notice, and Customer consents to such usage. The Privacy Notice does not apply to Customer Content.

3.3 Service Attributes. To provide billing and administration services, AWS may process Service Attributes in the AWS region(s) where Customer uses the Service Offerings and the AWS regions in the United States. To provide Customer with support services initiated by Customer and investigate fraud, abuse or violations of this Contract, AWS may process Service Attributes where AWS maintains its support and investigation personnel.

3.4 AWS Information Security Program. As of the Effective Date, the AWS Information Security Management System (ISMS) is ISO 27001 certified. AWS will maintain an information security program designed to provide at least the same level of protection as evidenced by that certification on the Effective Date.

3.5 Audits of Technical and Organizational Measures. Upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will provide to Customer a copy of the AWS System and Organization Controls 1, Type 2 report or such alternative industry standard reports or certifications that are substantially equivalent as reasonably determined by AWS. AWS will make this documentation available to Customer via AWS Artifact (or an alternative means accessible via the Contractor Site) and this documentation will be treated as Confidential Information of AWS under the NDA.

3.6 Regulatory Supervision. If a Regulator requires Customer to verify its compliance with applicable laws administered by the Regulator in connection with Customer's use of the Services (a "**Request**"), then AWS will assist Customer to address the Request as described in this Section.

(a) Information Requests. If Customer cannot satisfy a Request after using commercially reasonable efforts to do so (including by providing available information and documentation and access to the relevant AWS Enterprise Accounts) and notifies AWS of this condition, AWS will use commercially reasonable efforts to assist Customer to respond to the Request by providing (i) relevant information and documentation regarding the technical and organizational measures of AWS or its Affiliates and about this Agreement, and (ii) for those questions that cannot be satisfied by such information and documentation, if any, a security and compliance briefing by personnel of AWS or its Affiliates.

(b) On-Site Visit. Following a notice to AWS by a Regulator confirming its regulatory authority and that the Request cannot be satisfied by means that are less burdensome for AWS including pursuant to Section 3.5(a), AWS will permit a reasonable number of Regulator's compliance personnel or auditors to visit the premises of AWS or its Affiliates (a "**Visit**") for the purpose of assisting Customer to satisfy the Request. The Visit will be conducted in a manner that reasonably minimizes the disruption on the operations of AWS and its Affiliates.

(c) Confidentiality. Any assistance AWS provides under this Section 3.5 will be subject to AWS's applicable policies and reasonable limits related to safety, security, confidentiality, and maintaining the integrity of the AWS Network. Customer will undertake to obtain confidential treatment or similar protection for any information disclosed to, or gathered by, Regulator under this Section.

4. Customer Responsibilities.

4.1 Customer Content. Customer is solely responsible for the development, content, operation, maintenance, and use of Customer Content. Customer agrees that Customer Content will not violate any of the Policies or any applicable law.

4.2 Customer’s Security and Redundancy. Customers have a variety of options to choose from when configuring their accounts, and for all sensitive or otherwise valuable content AWS recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings in a manner that provides security and redundancy of its Contractor Enterprise Accounts and Customer Content, such as, for example, using enhanced access controls to prevent unauthorized access to Contractor Enterprise Accounts and Customer Content, using encryption technology to prevent unauthorized access to Customer Content, and ensuring the appropriate level of backup to prevent loss of Customer Content.

4.3 Log-In Credentials and Account Keys. AWS log-in credentials and private keys generated by the Services are for Customer’s internal use only and Customer may not sell, transfer or sublicense them to any other entity or person, except that Customer may disclose its private key to its agents and subcontractors (including any of its Affiliates who are acting as an agent or subcontractor of Customer) performing work on behalf of Customer. Except to the extent caused by AWS's breach of this Contract, as between the parties, Customer is responsible for all activities that occur under its Contractor Enterprise Accounts.

4.4 End Users. If Customer uses the Services to provide services to, or otherwise interact with, End Users, then Customer, and not AWS, will have the relationships (e.g., via executed contracts between Customer and End Users or via online terms of service) with End Users. Therefore Customer, and not AWS, is responsible for End Users' use of Customer Content and the Service Offerings. To the extent that Customer enables End Users to access the Services or Customer Content, Customer will ensure that all End Users comply with any applicable obligations of Customer under this Contract and that any terms of any agreement with each End User are not inconsistent with this Contract. AWS does not provide any support or services to End Users unless AWS has a separate agreement with Customer or an End User obligating AWS to provide support or services to End Users. Customer is responsible for providing customer service (if any) to End Users.

5. Fees and Payment.

5.1 Service Fees. Unless otherwise stated on the Contractor Site, AWS will invoice Customer at the end of each month for all applicable fees and charges accrued for use of the Service Offerings, as described on the Contractor Site, during the month. Customer will pay AWS all invoiced amounts within 45 days of the date of the invoice (other than Disputed Amounts). For any Disputed Amounts, Customer will provide Notice to AWS, including the basis for the dispute (including any supporting documentation), and the parties will meet within 30 days of the date of the Notice to resolve the dispute. All amounts payable by Customer under this Contract will be paid to AWS without setoff or counterclaim and without deduction or withholding, provided that Disputed Amounts will be handled as set forth above. Fees and charges for any new Service or new feature of a Service will be effective when AWS posts updated fees and charges on the Contractor Site, unless expressly stated otherwise in a Notice. AWS may increase or add new fees and charges for any existing Service by giving Customer at least 60 days' prior Notice.

5.2 Taxes. Each party will be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that party upon or with respect to the transactions and payments under this Contract. All fees payable by Customer are exclusive of Indirect Taxes, except where applicable law requires otherwise. AWS may charge and Customer will pay applicable Indirect Taxes that AWS is legally obligated or authorized to collect from Customer. Customer will provide such information to AWS as reasonably required to determine whether AWS is obligated to collect Indirect Taxes from Customer. AWS will not collect, and Customer will not pay, any Indirect Tax for which Customer furnishes AWS a properly completed exemption certificate or a direct payment permit certificate for which AWS may claim an available exemption from such Indirect Tax. All payments made by Customer to AWS under this Contract will be made free and clear of any deduction or withholding, as may be required by law. If any such deduction or withholding (including but not limited to cross-border withholding taxes) is required on any payment, Customer will pay such additional amounts as are necessary so that the net amount received by AWS is equal to the amount then due and payable under this Contract. AWS will provide Customer with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Contract.

6. Temporary Limitation of Access and Use Rights. AWS may temporarily limit (in full or in part, as set forth in this Section 6) Customer's or any End User's right to access or use the Service Offerings upon Notice to Customer (which will be reasonable prior notice unless AWS reasonably believes immediate limitation is necessary) if AWS reasonably determines that Customer's or an End User's use of the Service Offerings poses a security risk or threat to the function of the Service Offerings, or poses a security or liability risk or threat of harm to AWS, its Affiliates or any third party. AWS will only limit Customer's right to access or use the instances, data or portions of the Service Offerings that caused the security or liability risk or threat. AWS will restore Customer's access and use rights promptly after Customer has resolved the issue giving rise to the limitation. Customer remains responsible for all fees and charges for the Service Offerings during the period of limitation.

7. Term; Termination.

7.1 Term. The term of this Contract will commence on the Effective Date and will remain in effect until terminated pursuant to this Contract. Any Notice of termination of this Contract must include a Termination Date.

7.2 Termination

(a) Termination for Convenience. Customer may terminate this Agreement for any reason by providing AWS Notice. AWS may terminate this Agreement for any reason by providing Customer at least two years' Notice.

(b) Termination for Cause.

(i) By Customer or Contractor. Either Customer or AWS may terminate this Agreement for cause if the other is in material breach of this Agreement and the material breach remains uncured for a period of 30 days from receipt of Notice by the breaching party.

(ii) By AWS. AWS may terminate this Agreement for cause (a) upon 90 days' Notice to Customer if AWS has the right to limit Customer's or any End User's right to access or use the Service Offerings under Section 6 and Customer has not cured the condition giving rise to that right to limit within such 90 day period, or (b) upon 30 days' Notice to Customer in order to comply with applicable law or requirements of governmental entities.

7.3 Effect of Termination.

(a) Generally. Upon the Termination Date:

(i) except as provided in 7.3(b) and the Addendum, all of Customer's rights under this Contract immediately terminate;

(ii) Customer remains responsible for all fees and charges Customer has incurred through the Termination Date;

(iii) Customer will immediately return or, if instructed by Contract, destroy all Contractor Content in Customer's possession (except for Contractor Content that is publicly available on the AWS Site); and

(iv) Sections 4 (Customer Responsibilities), 5 (Fees and Payment), 7.3 (Termination), 8.1 (Customer Content), 8.2 (Proprietary Rights), 8.3 (License Restrictions), 8.4 (Suggestions), 9 (Third Party Claims), 10.3 (Warranty Disclaimers), 11 (Limitations of Liability), 12 (Miscellaneous) and 13 (Definitions) will continue to apply and survive in accordance with their terms.

(b) Post-Termination Retrieval of Customer Content. During the 90 days following the Termination Date, AWS will not take action to remove any Customer Content as a result of the termination from any AWS Enterprise Account that is open on the Termination Date. In addition, during such period, AWS will allow Customer to retrieve any remaining Customer Content from the Services, unless (i) prohibited by law or the order of a governmental or regulatory body or it could subject AWS or its Affiliates to liability, or (ii) Customer has not paid all amounts due under this Agreement, other than Disputed Amounts. For any use of the Services during such period, the terms of this Agreement will apply and Customer will pay the applicable fees at the rates under Section 5 (including, without limitation, applicable fees for storage). No later than the end of this 90 day period, Customer will close all AWS Enterprise Accounts.

8. Proprietary Rights.

8.1 Customer Content. As between Customer and Contractor, Customer (or Customer's licensors) own all right, title, and interest in and to Customer Content. Except as provided in this Agreement, Contractor obtains no rights under this Agreement from Customer (or Customer's licensors) to Customer Content.

8.2 Service Offerings License. Contractor or its licensors own all right, title, and interest in and to the Service Offerings, and all related technology and intellectual property rights. Subject to the terms of this Agreement, Contractor grants Customer a limited, revocable, non-exclusive, non-sublicensable, non-transferrable license to do the following: (a) access and use the Services solely in accordance with this Agreement; and (b) copy and use the Contractor Content solely for Customer's permitted use of the Services. Except as provided in this Section 8.2, Customer obtains no rights under this Agreement from AWS, its Affiliates, or their licensors to the Service Offerings, including without limitation any related intellectual property rights. Some Contractor Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, which will be identified to Customer in the notice file or on the download page, in which case that license will govern Customer's use of that Contractor Content.

8.3 License Restrictions. Neither Customer nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted by this Agreement. Neither Customer nor any End User may, or may attempt to (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content included in the Service Offerings (except to the extent Content included in the Service Offerings is provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the Service Offerings or apply any other process or procedure to derive the source code of any software included in the Service Offerings, (c) access or use the Service Offerings in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (d) resell or sublicense the Service Offerings. Customer may only use the Contractor Marks in accordance with the Trademark Use Guidelines. Customer will not misrepresent or embellish the relationship between Contractor and Customer (including by expressing or implying that Contractor supports, sponsors, endorses, or contributes to Customer or Customer's business endeavors). Customer will not imply any relationship or affiliation between Contractor and Customer except as expressly permitted by this Agreement.

8.4 Suggestions. If Customer elects to provide any Suggestions to Contractor or its Affiliates, Contractor and its Affiliates will be entitled to use the Suggestions without restriction.

9. Third-Party Claims.

9.1 Policies and Harm to Third Parties. Customer represents and warrants that (i) Customer's and its End Users' access and use of the Service Offerings will not violate the Policies, and

(ii) Customer's access and use of the Service Offerings will not cause harm to any third party, including End Users.

9.2 Intellectual Property.

(a) Subject to the limitations in this Section 9, AWS will defend Customer and its employees, officers, and directors against any third-party claim alleging that the Services infringe or misappropriate that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(b) Subject to the limitations in this Section 9, Customer represents and warrants that Customer Content will not infringe or misappropriate any third party's intellectual property rights.

(c) No party will have obligations or liability under this Section 9.2 arising from infringement by combinations of the Services or Customer Content, as applicable, with any other product, service, software, data, content, or method. In addition, AWS will have no obligations or liability arising from Customer's or any End User's use of the Services after AWS has notified Customer to discontinue such use. The remedies provided in this Section 9.2 are the sole and exclusive remedies for any third-party claims of infringement or misappropriation of intellectual property rights by the Services or by Customer Content.

(d) For any claim covered by Section 9.2(a), AWS will, at its election, either: (i) procure the rights to use that portion of the Services alleged to be infringing; (ii) replace the alleged infringing portion of the Services with a non-infringing alternative; (iii) modify the alleged infringing portion of the Services to make it non-infringing; or (iv) terminate the allegedly infringing portion of the Services or this Contract.

9.3 Third-Party Claims arising from a Data Security Incident. Subject to the limitations in Section 9 of the Enterprise Agreement, AWS will defend Customer and its employees, officers and directors against any third-party claim arising from a Data Security Incident, and AWS will pay the amount of any resulting adverse final judgment or settlement. THE AGGREGATE LIABILITY OF AWS, TOGETHER WITH ITS AFFILIATES, UNDER THIS SECTION 1.11 (INCLUDING LIABILITY TO ALL CUSTOMER AFFILIATES USING THE SERVICES UNDER SECTION 1.4 OF THE ENTERPRISE AGREEMENT) WILL NOT EXCEED $25,000,000. THIS SECTION 1.11 PROVIDES THE EXCLUSIVE REMEDIES UNDER THIS AGREEMENT FOR ANY THIRD-PARTY CLAIM ARISING FROM A DATA SECURITY INCIDENT.

9.4 Process. The obligations under Section 9.2(a) will apply only if Customer: (a) gives AWS prompt Notice of the claim; (b) permits AWS to control the defense and settlement of the claim; and (c) reasonably cooperates with AWS (at AWS's expense) in the defense and settlement of the claim. In no event will AWS agree to any settlement of any claim that involves any commitment, other than the payment of money, without the written consent of Customer.

10. Contractor Warranties and Warranty Disclaimers.

10.1 Contractor Warranties. Contractor represents and warrants to Customer that the Services will perform substantially in accordance with the Documentation.

10.2 Mutual Warranties. Customer and Contractor each represents and warrants to the other that (a) it has full power and authority to enter into and perform this Agreement, (b) the execution and delivery of this Agreement has been duly authorized, (c) it will comply with all applicable laws, rules, regulations and ordinances in the performance of this Agreement (and, in the case of Customer, the use of the Service Offerings), and (d) its performance hereunder does not breach any other agreement to which it is bound.

10.3 Warranty Disclaimers. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 10.1 AND SECTION 10.2, AND EXCEPT TO THE EXTENT PROHIBITED BY LAW, CONTRACTOR, ITS AFFILIATES AND ITS LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND DISCLAIM ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (A) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (B) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (C) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (D) THAT ANY CONTENT, INCLUDING CUSTOMER CONTENT OR THIRD-PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

11. Limitations of Liability

11.1 Liability Disclaimers. EXCEPT FOR PAYMENT OBLIGATIONS ARISING UNDER SECTION 9.1, NEITHER AWS NOR CUSTOMER, NOR ANY OF THEIR AFFILIATES OR LICENSORS, WILL BE LIABLE TO THE OTHER UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR (A) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, (B) THE VALUE OF CUSTOMER CONTENT, (C) LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, OR GOODWILL, OR (D) UNAVAILABILITY OF THE SERVICE OFFERINGS (THIS DOES NOT LIMIT ANY SERVICE CREDITS THAT MAY BE AVAILABLE UNDER SERVICE LEVEL AGREEMENTS).

11.2 Damages Cap. EXCEPT FOR PAYMENT OBLIGATIONS ARISING UNDER SECTION 9, THE AGGREGATE LIABILITY UNDER THIS AGREEMENT OF AWS, AND ANY OF ITS RESPECTIVE AFFILIATES OR LICENSORS, WILL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO AWS UNDER THIS AGREEMENT FOR THE SERVICES THAT GAVE RISE TO THE LIABILITY DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE; PROVIDED, HOWEVER THAT NOTHING IN THIS SECTION 11 WILL LIMIT CUSTOMER'S OBLIGATION TO PAY AWS FOR CUSTOMER'S USE OF THE SERVICE OFFERINGS PURSUANT TO SECTION 5, OR ANY OTHER PAYMENT OBLIGATIONS UNDER THIS AGREEMENT.

11.3 Specified Damages Cap for a Data Security Incident. Specified Damages incurred by Customer as a result of a Data Security Incident are not disclaimed under Enterprise Agreement Section 11.1. SUBJECT TO SECTION 11.2 of the ENTERPRISE AGREEMENT, THE AGGREGATE LIABILITY OF AWS, TOGETHER WITH ITS AFFILIATES, FOR SPECIFIED DAMAGES UNDER THIS AGREEMENT (INCLUDING LIABILITY TO ALL CUSTOMER AFFILIATES USING THE SERVICES UNDER SECTION 1.4 OF THE ENTERPRISE AGREEMENT) WILL NOT EXCEED $25,000,000.

12. Miscellaneous.

12.1 Assignment. Neither Customer nor AWS may assign or otherwise transfer this Agreement or any of its rights and obligations under this Agreement without the prior written approval of the other; except that either Customer or AWS may assign or otherwise transfer this Agreement without the consent of the other (a) in connection with a merger, acquisition or sale of all or substantially all of its assets, or (b) to any Affiliate or as part of a corporate reorganization, or (c) in the case of AWS, with respect to specific AWS Enterprise Accounts, to an Affiliate. Effective upon such assignment or transfer, subject to the assignee/transferee's consent, the assignee/transferee is deemed substituted for the assignor/transferor as a party to this Agreement and the assignor/transferor is fully released from all of its obligations and duties to perform under this Agreement. Subject to the foregoing, this Agreement will be binding upon, and inure to the benefit of the parties and their respective permitted successors and assigns.

12.2 Counterparts; Facsimile. This Agreement may be executed by facsimile or by electronic signature in a format approved by AWS, and in counterparts, each of which (including signature pages) will be deemed an original, but all of which together will constitute one and the same instrument.

12.3 Entire Agreement. This Agreement incorporates the Policies and is made part of the Contract. The Contract supersedes all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS, whether written or verbal, regarding the subject matter of the Contract (including, as set forth in Section 1.2, any acceptance of the AWS Customer Agreement by Customer or any of its employees acting on behalf of Customer). AWS will not be bound by any term, condition or other provision which is different from or in addition to the provisions of this Contract (whether or not it would materially alter this Contract) including but not limited to, for example, any term, condition or other provision submitted by Customer in any order, receipt, acceptance, confirmation, correspondence or other document, related to any invoicing process that Customer submits or requires AWS to complete, etc. If the terms of this Agreement are inconsistent with the terms of any attachment or any Policy then the terms of this Agreement will control except that Addendum 1: Contractor Terms for Cloud and Infrastructure as a Service (IAAS) Products will control over any conflicting terms in this Agreement. No modification or amendment of any portion of this Contract will be effective unless in writing and signed by the parties to this Contract.

12.4 Force Majeure. Except for payment obligations, no party will be liable for any delay or failure to perform any obligation under this Contract where the delay or failure results from any cause beyond its reasonable control, including acts of God, labor disputes or other industrial disturbances, electrical or power outage, utilities or telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

12.5 Reserved.

12.6 Trade Compliance. In connection with this Contract, each party will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control. Customer is solely responsible for compliance with applicable laws related to the manner in which Customer chooses to use the Service Offerings, including (i) Customer's transfer and processing of Customer Content, (ii) the provision of Customer Content to End Users, and (iii) specifying the AWS region in which any of the foregoing occur. Customer represents that Customer and the entities that own or control Customer, and the financial institutions used to pay AWS under this Contract, are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the U.S. Department of Treasury's Specially Designated Nationals list and Foreign Sanctions Evaders list, and the U.S. Department of Commerce's Entity List), the European Union or its member states, or other applicable government authority.

12.7 Independent Contractors. AWS and Customer are independent contractors, and this Agreement will not be construed to create a partnership, joint venture, agency, or employment relationship. Neither Customer nor AWS, nor any of their respective Affiliates, is an agent of the other for any purpose or has the authority to bind the other.

12.8 Language. All communications and Notices made or given pursuant to this Contract must be in the English language. If AWS provides a translation of the English language version of this Contract, the English language version of the Contract will control if there is any conflict.

12.9 Nondisclosure. If the parties have an NDA, then the NDA is incorporated by reference into this Contract, except that the security provisions in Section 3, not the NDA, apply to Customer Content. Except to the extent permitted by applicable law, neither Customer nor AWS will issue any press release or make any other public communication with respect to this Agreement or Customer's use of the Service Offerings. AWS and Customer agree that the contents of this Agreement are not publicly known and will not be disclosed by them.

12.10 Notice.

(a) General. Except as otherwise set forth in Section 12.6(b), to give notice to a party under this Contract, each party must contact that other party as follows: (i) by facsimile transmission; or (ii) by personal delivery, overnight courier or registered or certified mail. Notices must be sent to the fax number of the other party listed on the Cover Page to this Contract or addressed to the address of the other party listed on the Cover Page to this Contract. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three business days after they are sent.

(b) Electronic Notice. AWS may provide notice to Customer (i) under Sections 2.2 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6 or Attachment A by sending a message to the email address then associated with Customer's applicable AWS Enterprise Account, and (iii) under Section 2.1 by sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will be effective upon posting and notices provided by email will be effective when AWS sends the email.

12.11 No Third-Party Beneficiaries. Except as set forth in Section 9, this Agreement does not create any third-party beneficiary rights in any individual or entity that is not a party to this Agreement.

12.12 No Waivers. The failure by a party to enforce any provision of this Contract will not constitute a present or future waiver of such provision nor limit such party's right to enforce such provision at a later time. All waivers by a party must be provided in a Notice to be effective.

12.13 Severability. If any portion of this Agreement is held to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect. Any invalid or unenforceable portions will be interpreted to give effect to the intent of the original portion. If such construction is not possible, the invalid or unenforceable portion will be severed from this Agreement but the rest of the Agreement will remain in full force and effect.

13. Definitions. Defined terms used in this Contract with initial letters capitalized have the meanings given below:

"Acceptable Use Policy" means the policy located at http://aws.amazon.com/aup (and any successor or related locations designated by AWS), as it may be updated by AWS from time to time.

"Account Information" means information about Customer that Customer provides to AWS in the creation or administration of an AWS Enterprise Account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with an AWS Enterprise Account.

"Affiliate" means any entity that directly or indirectly controls, is controlled by or is under common control with that party.

“API” means an application program interface.

“AWS Content” means Content that AWS or any of its Affiliates makes available related to the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; sample code; software libraries; command line tools; proofs of concept, templates, and other related technology (including but not limited to any of the foregoing that are provided by any AWS personnel). AWS Content does not include the Services or Third-Party Content.

“AWS Contracting Party” means each party identified on the AWS Contracting Party Site that is or becomes a party to this Agreement.

“AWS Contracting Party Site” means https://aws.amazon.com/legal/aws-contracting-party (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“AWS Customer Agreement” means AWS’s standard user agreement located on the AWS Site at http://aws.amazon.com/agreement (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“AWS Enterprise Account” means any AWS account that (a) is listed on Attachment A, as that list may be updated from time to time as described in Attachment A, (b) is opened by Customer using a Customer-issued email address (with an email domain name that is owned by Customer), (c) includes Customer’s full legal name in the “Company Name” field associated with the AWS account, and (d) is associated with a geographic location that corresponds to an AWS Contracting Party that is a party to this Agreement, as set forth in Section 12.14.

“AWS Marks” means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its Affiliates that AWS may make available to Customer in connection with this Agreement.

“AWS Network” means AWS’s data center facilities, servers, networking equipment, storage media, and host software systems (e.g., virtual firewalls, access software, and hypervisors, etc.) that are within AWS’s control and are used to provide the Services.

“AWS Security Standards” means the security standards attached to this Agreement as Attachment B.

"**AWS Services**" means all the generally available services made available by AWS or its Affiliates, through the AWS Management Console (or through other means by which AWS makes such services available).

“AWS Site” means http://aws.amazon.com (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Content” means software (including machine images), data, text, audio, video, or images.

“Customer Content” means Content that Customer or any End User transfers to AWS for processing, storage or hosting by the Services in connection with an AWS Enterprise Account and any computational results that Customer or any End User derive from the foregoing through its use of the Services. For example, Customer Content includes Content that Customer or any End User stores in Amazon Simple Storage Service. Customer Content does not include Account Information.

“Data Security Incident” means unauthorized access to Customer Content by a third party caused by a material breach by AWS of its obligations under Section 3.1, provided that Customer has complied with the Minimum Architecture Requirements.

“Disputed Amounts” means amounts disputed by Customer in a Notice and in good faith as billing errors.

“Documentation” means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services located at http://aws.amazon.com/documentation (and any successor or related locations designated by AWS), as such user guides and admin guides may be updated by AWS from time to time.

“End User” means any individual or entity that directly or indirectly through another user (a) accesses or uses Customer Content, or (b) otherwise accesses or uses the Service Offerings under an AWS Enterprise Account. The term “End User” does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than under an AWS Enterprise Account.

“Indirect Taxes” means applicable taxes and duties, including, without limitation, VAT, GST, excise taxes, sales and transactions taxes, and gross receipts tax.

“Losses” means any damages, losses, liabilities, costs and expenses (including reasonable attorneys’ fees).

“Minimum Architecture Requirements” means the requirements in Attachment C.

“NDA” means the Mutual Nondisclosure Agreement between Customer and Amazon.com, Inc., dated November 9, 2021.

“Notice” means any notice provided in accordance with Section 12.10.

“Policies” means the Acceptable Use Policy, Privacy Notice, and the Service Terms.

“Privacy Notice” means the privacy notice located at http://aws.amazon.com/privacy (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"Regulated End User" means an End User who is supervised by a Regulator.

"Regulator" means a government or regulatory body with binding authority to regulate Customer's services activities; provided, that the term Regulator does not include any regulatory body or instrumentality of Iran, North Korea, the People's Republic of China or of any country that is subject to embargo or sanction by the United States as administered by the Office of Foreign Assets Control (OFAC).

“Service” means each of the services made available by AWS or its Affiliates for which Customer registers via the AWS Site (or by such other means made available by AWS), including those web services described in the Service Terms. Services do not include Third-Party Content.

“Service Attributes” means Service usage data related to an AWS Enterprise Account, such as resource identifiers, metadata tags, security and access roles, rules, usage policies, permissions, usage statistics and analytics.

“Service Level Agreement” means all service level agreements that AWS offers with respect to the Services and post on the AWS Site, as they may be updated by AWS from time to time. The service level agreements that AWS offers with respect to the Services are located at https://aws.amazon.com/legal/service-level-agreements (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Service Offerings” means the Services, the AWS Content, the AWS Marks, and any other product or service provided by AWS under this Agreement. Service Offerings do not include Third-Party Content.

“Service Terms” means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Specified Damages” means (1) Customer’s commercially reasonable out-of-pocket costs to provide legally required notification to its affected customers, (2) Customer’s commercially reasonable out-of-pocket costs to provide up to 12 months of credit monitoring services for its affected customers that Customer is legally required to notify, and (3) the amount of any regulatory fines and penalties Customer is required to pay.

“Suggestions” means all suggested improvements to the Service Offerings that Customer provides to AWS.

“Term” means the term of this Agreement described in Section 7.1.

“Termination Date” means the effective date of termination provided in a Notice in accordance with Section 7.

“Third-Party Content” means Content of a third party made available on the AWS Marketplace or on developer forums, sample code repositories, public data repositories, community-focused areas of the

AWS Site, or any other part of the AWS Site that allows third parties to make available software, products, or data.

“Trademark Use Guidelines” means the guidelines and trademark license located at http://aws.amazon.com/trademark-guidelines/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

Attachment A

AWS Account ID(s):

The list above includes any Master Account or Member Accounts joined to such accounts via AWS Organizations, as described in the Service Terms.

Customer may add AWS accounts to the list above or remove AWS accounts from the list above by providing notice to AWS via email to enterprise-accounts@amazon.com, that includes (1) Customer's full name, in the form of "CUST-[____________]", (2) the Enterprise Agreement number (which begins with "CC" and is found on the upper right corner of each page of this Agreement), and (3) the AWS Account ID of each added or removed AWS account. Upon Notice, AWS may replace the notification process or make available another means of adding and removing AWS accounts to the list above.

Attachment B - Contractor Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable Customer Enterprise Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

3. Security Event Notification. If AWS knows of a breach of the security measures described in these Contractor Security Standards that resulted in either (a) any unlawful access to any Customer Content stored on AWS's equipment or in AWS's facilities, or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of Customer Content (each a "Security Event"), AWS will promptly: (x) notify Customer of the Security Event; and (y) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Event.

ATTACHMENT C – MINIMUM ARCHITECTURE REQUIREMENTS

Each reference in this Attachment to specific Services includes equivalent alternative or replacement Service(s) that AWS makes available. At all times Customer will comply with all of the following:

1. **Encryption.** Encrypt all Customer Content in transit and at rest, using Strong Cryptography with associated key management processes and procedures. "**Strong Cryptography**" has the meaning given in Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms, Version 3.2 (as updated from time to time).

2. **Security Architecture.**

   (a) Promptly address any security and privacy events as notified at http://aws.amazon.com/security/security-bulletins/, except those categorized as "Informational."

   (b) Monitor and evaluate software running in its AWS Enterprise Accounts for known and new vulnerabilities and take the steps necessary to address such vulnerabilities.

3. **Access Management.**

   (a) Use multi-factor authentication to control access to root account credentials and not use root account credentials beyond initial account configuration, except in using Services for which AWS Identity and Access Management (IAM) is not available.

   (b) Require each user to have unique security credentials that are rotated at least quarterly.

   (c) Use multifactor authentication or federated credentials for all authentications and grant users and groups only the minimum privileges necessary.

   (d) Restrict permissions in Security Groups and Access Control Lists to only those users required for Customer's use of the Services.

   (e) Restrict permitted source and destination authorizations to only those required for Customer's use of the Services.

   (f) Apply resource-based policies to limit access to Services only to authorized parties.

4. **Backup and Redundancy.**

   (a) Back up Customer Content in accordance with industry-standard security configurations.

   (b) Store all Customer Content redundantly in more than one AWS Region

ADDENDUM 1 - CONTRACTOR TERMS FOR CLOUD AND INFRASTRUCTURE AS A SERVICE (IAAS) PRODUCTS

This Addendum together with its Schedules, Exhibits and any other applicable attachments is hereby incorporated by reference into and made part of the underlying agreement dated December 6, 2022 (Collectively this "Contract") between the State of Michigan (the "**State**" or "**Customer**") and Amazon Web Services Inc. ("**Contractor**"), a Delaware corporation. This Addendum is effective on December 6, 2022 ("**Effective Date**"), and unless terminated, will expire on December 6, 2027 (the "**Term**"). The State is seeking to consume Services for the purpose of provision processing, storage, networks, and other fundamental computing resources where the State is able to deploy and run arbitrary software, which can include operating systems and applications.

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

1. The below terms and conditions of this Addendum (including all Schedules, Exhibits and attachments hereto) shall prevail and govern in the case of any inconsistency or conflict with the terms and conditions of any other document that relates to the purchase of Contractor's products and services that form the contractual relationship between the parties, including but not limited to any master agreement to which the Addendum applies or any agreement, schedule, or other attachment referenced by link or otherwise provided on Contractor's website. Notwithstanding anything to the contrary in Contractor's terms to which this Addendum is attached/incorporated or on Contractor's website(s) related to the purchased products, the following terms and conditions apply with respect to the State:

1.1 Upon notice to Contractor, the State, in its sole discretion, may assign in whole, its rights or responsibilities under this Contract to any other State of Michigan government agency. 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.

1.2 Subcontracting. Contractor will be responsible and liable for the acts and omissions of each subcontractor (including such subcontractor's employees) to the same extent as if such acts or omissions were by Contractor or its employees. Contractor is responsible for all fees and expenses payable to, by or on behalf of each subcontractor in connection with this Contract. Contractor must provide the State with a list of Chain Subcontractors that is accessible for review by the State.

1.3 Payment. 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. Undisputed invoices will be due and payable by the State, in accordance with the State's Prompt Payment Act as specified in 1984 PA 279, MCL 17.51 et seq., within 45 days after receipt, provided the State determines that the invoice was properly rendered. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if the Services purchased are for the State's exclusive use. The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. Contractor shall not withhold any Services or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this Section. 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. Contractor's acceptance of final payment of all invoiced disputed and undisputed amounts by the State constitutes a waiver of claims for non-payment by Contractor against the State. Any undisputed amounts not paid by the State when due for Contract Activities received may be assessed overdue account charges up to a maximum rate of 0.75% per month on the outstanding balance pursuant to 1984 PA 279, MCL 17.51, *et seq*.

1.4 Termination for Public Interest. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. If the State terminates the Contract for the Public Interest, the State will not be responsible for any early termination fees, acceleration clauses, minimum purchase amounts, or any other requirement on the State to expend additional funds beyond those undisputed amounts already due and payable to Contractor to the extent that funds explicitly appropriated for that purpose are available for any Service Offerings used after termination.

1.5 Transition Responsibilities.

i) End of Contract.

(1) Upon termination or expiration of this Contract, for any reason, Contractor must, for a period of time specified by the State (not to exceed 180 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to:

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

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

(c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with the terms of this Addendum regarding the destruction of Customer Data at the conclusion of the Transition Period; and make available an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**").

(2) Transition Assistance Upon Termination or Expiration of the Contract, during the Transition Period, Customer may make a written request for advisory and implementation services from Contractor to assist in migrating workloads and applications or otherwise transitioning Customer's use of the Services ("Transition Assistance"). Contractor will provide Transition Assistance to Customer subject to the Implementation Services Schedule or such other agreement between Contractor and Customer under which Contractor agrees to provide advisory and implementation services to Customer. These terms will describe the scope of the Transition Assistance and any applicable fees.

1.6 Indemnification Procedure. Pursuant to MCL 14.28 and MCL 14.29, 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

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

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

1.9 Limitation of Liability. EXCEPT AS PROVIDED IN SECTION 1.10, IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY 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 FEES PAID BY THE STATE TO CONTRACTOR FOR THE RELEVANT PRODUCT DURING THE TWELVE (12) MONTH PERIOD BEFORE THE EVENT GIVING RISE TO THE LIABILITY.

1.10Specified Damages Cap for a Data Security Incident. Specified Damages incurred by Customer as a result of a Data Security Incident are not disclaimed under Enterprise Agreement Section 11.1. SUBJECT TO SECTION 11.2 of the ENTERPRISE AGREEMENT, THE AGGREGATE LIABILITY OF AWS, TOGETHER WITH ITS AFFILIATES, FOR SPECIFIED DAMAGES UNDER THIS AGREEMENT (INCLUDING LIABILITY TO ALL CUSTOMER AFFILIATES USING THE SERVICES UNDER SECTION 1.4 OF THE ENTERPRISE AGREEMENT) WILL NOT EXCEED $25,000,000.

1.11 Third-Party Claims arising from a Data Security Incident. Subject to the limitations in Section 9 of the Enterprise Agreement, AWS will defend Customer and its employees, officers and directors against any third-party claim arising from a Data Security Incident, and AWS will pay the amount of any resulting adverse final judgment or settlement. THE AGGREGATE LIABILITY OF AWS, TOGETHER WITH ITS AFFILIATES, UNDER THIS SECTION 1.11 (INCLUDING LIABILITY TO ALL CUSTOMER AFFILIATES USING THE SERVICES UNDER SECTION 1.4 OF THE ENTERPRISE AGREEMENT) WILL NOT EXCEED $25,000,000. THIS SECTION 1.11 PROVIDES THE EXCLUSIVE REMEDIES UNDER THIS AGREEMENT FOR ANY THIRD-PARTY CLAIM ARISING FROM A DATA SECURITY INCIDENT.

1.12 The State is statutorily obligated to comply with the Michigan Freedom of Information Act, MCL 15.231 *et seq.* (FOIA). The State will not be liable for any breach of any conflicting requirements found in this Contract, any Contractor websites, portals, ordering documents, or any other representations when acting in compliance with the FOIA and Addendum Section 2.2.

1.13 Pursuant to MCL 18.1470, the State or its designee may audit Contractor to verify compliance with this Contract.

1.14 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.

1.15 The State will not be bound by any terms requiring indemnification by the State to third- parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to State systems; agreeing to be bound by the laws of another state; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the product-specific end user license agreements (EULA(s)) or any other documents, policies, or terms located in links referenced herein.

2. Contractor Requirements. Notwithstanding anything to the contrary in in this Contract, any Contractor websites, portals, ordering documents, or any other representations, Contractor agrees that:

2.1 Contractor Use of Customer Data. Contractor is provided a limited license to Customer Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display Customer Data only to the extent necessary in the provision of the Services. This license expires at the expiration or termination of the Contract. Contractor must:

(a) keep and maintain Customer 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 Customer 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) enable the State to select Service Offerings that will keep and maintain Customer Data in the continental United States; and

(d) not use, sell, rent, transfer, distribute, commercially exploit, or otherwise disclose or make available Customer 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 Customer Data may violate state or federal laws, including but not limited to MCL 752.795.

2.2 Legal Process. If the Recipient receives Legal Process for the Disclosing Party's Confidential Information, the Recipient will: (a) promptly notify the Disclosing Party prior to such disclosure unless the Recipient is legally prohibited from doing so; (b) attempt to redirect the third party to request it from the Disclosing Party directly; (c) comply with the Disclosing Party's reasonable requests to oppose disclosure of its Confidential Information, provided however, that the State will disclose information in accordance with the Michigan Freedom of Information Act, MCL 15.231; and (d) use commercially reasonable efforts to object to, or limit or modify, any Legal Process that the Recipient reasonably determines is overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. To facilitate the request in (b), the Recipient may provide the Disclosing Party's basic contact information to the third party.

"Legal Process" means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, or other valid legal authority, legal procedure, or similar process.

2.3 Contractor agrees that, if the State determines that State or federal rules or regulations require the appendage of specific contractual language in contracts related to specific types of data, including by not limited CJIS and IRS/FTI data, Contractor will append such required contractual language, as mutually agreed by the parties, to this Contract before purchase by the State of the relevant product is completed, if Contractor is notified by the State prior to purchase that additional language may be required. In the event the Contractor, in its sole discretion, determines that it cannot comply with the required contractual language, the workloads shall not be part of the scope ("out of scope workloads". If the Contractor, in its sole discretion, determines it can comply with the required contractual language, the workloads shall be considered "in-scope workloads." Contractor understands that failure to append such required contractual language for in-scope workloads may subject the State to negative audit findings, and as such failure to append such required contractual language for in-scope workloads, may result in an indemnification request from the State. Further, failure to append contractual language for in-scope workloads related to specific types of data and required by federal rules or regulations such required contractual language shall be deemed a material breach of this Contract by Contractor.

2.4 Loss or Compromise of Data. If Contractor fails to comply with its security and privacy terms, as set forth in this Contract or on any associated Contractor websites, portals, ordering documents, or any other representations, and such failure results in (a) a compromise of the security, confidentiality, or integrity of Customer 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 Customer Data; (b) any unlawful access to any Customer Content stored on AWS's equipment or in AWS's or Chain Subcontractor's facilities; or (c) any unauthorized access to such equipment or facilities, where in any case such access results in or AWS reasonably believes such access will likely results in loss, disclosure, or alteration of Customer Content , Contractor must, as applicable:

(a) unless otherwise required for compliance with federal regulatory requirements, legal requirement or law, and provided that State is enrolled in Contractor's On-Ramp or Enterprise-level Support plan notify the State as soon as practicable but no later than twenty-four (24) hours of confirming of a Security Event;

(b) cooperate with the State in investigating the occurrence, including making available a root cause analysis ("**RCA**") of the event. The RCA typically provides AWS's determination of the cause of the Security Event and the remediation efforts taken or underway to prevent the conditions giving rise to the Security Event from recurring. The State agrees that it will treat the RCA as Contractor's Confidential Information. If the Michigan Security Operations Center (MISOC) requests additional information, Contractor agrees to work in good faith with MISOC to gather the information requested. The request for additional information is subject to the Contractor's standard commercial practices, including not providing information about other customers.

(c) If a Regulator requires Customer to verify its compliance with applicable laws administered by the Regulator in connection with Customer's use of the Services (a "**Request**"), then AWS will assist Customer to address the Request as described in this sub-section.

(i) **Information Requests**. If Customer cannot satisfy a Request after using commercially reasonable efforts to do so (including by providing available information and documentation and access to the relevant AWS Enterprise Accounts) and notifies AWS of this condition, AWS will use commercially reasonable efforts to assist Customer to respond to the Request by providing (i) relevant information and documentation regarding the technical and organizational measures of AWS or its Affiliates and about this Agreement, and (ii) for those questions that cannot be satisfied by such information and documentation, if any, a security and compliance briefing by personnel of AWS or its Affiliates.

(ii) **On-Site Visit.** Following a notice to AWS by a Regulator confirming its regulatory authority and that the Request cannot be satisfied by means that are less burdensome for AWS including pursuant to Section 3.5(a) of the Enterprise Agreement, AWS will permit a reasonable number of Regulator's compliance personnel or auditors to visit the premises of AWS or its Affiliates (a "**Visit**") for the purpose of assisting Customer to satisfy the Request. The Visit will be conducted in a manner that reasonably minimizes the disruption on the operations of AWS and its Affiliates.

(iii) **Confidentiality.** Any assistance AWS provides under this Section 3.5 of the Enterprise Agreement will be subject to AWS's applicable policies and reasonable limits related to safety, security, confidentiality, and maintaining the integrity of the AWS Network. Customer will undertake to obtain confidential treatment or similar protection for any information disclosed to, or gathered by, Regulator under this Section.

(d) in the case of PII or PHI, reimburse the State for any reasonable costs in notifying the affected individuals subject to Addendum Section 1.10 - Contractor's Specified Damages Cap for a Data Security Incident;

(e) 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 twenty-four (24) months following the date of notification to such individuals, subject to Addendum Section 1.10 - Contractor's Specified Damages Cap for a Data Security Incident;

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

(g) 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, subject to Addendum Section 1.10 - Contractor's Specified Damages Cap for a Data Security Incident;

(h) 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, subject to Section 1.11 - Third-Party Claims arising from a Data Security Incident;

(i) to the extent that Customer has chosen a product that provides for the backup and restoration of Customer Data, (i) enable Customer to restore backed up Customer Data in accordance with the Documentation; (ii) Contractor is liable if Customer Data is lost due to Contractor's breach of its warranty as set forth in Contractor's Enterprise Agreement;

(j) Unless otherwise set forth in this Addendum, Contractor will notify Customer of a Security Event in accordance with the process and timelines set out in the Data Processing and Security Terms. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address; and

(k) The parties agree that any damages relating to a breach of Contractor's obligations related to security and privacy are to be considered direct damages and not consequential damages.

2.5 This Section, and any other section where enforcement after the term of the Contract may reasonably be necessary, survives termination or expiration of this Contract.at all times in connection with its actual or required provision of services as purchased by the State pursuant to this Contract, Contractor will maintain and enforce an information security and privacy programs, including safety and physical and technical security policies and procedures with respect to its processing of the Customer Data, as set forth in any Contractor websites, portals, ordering documents, or any other representations;

(a) Data Privacy and Information Security. Throughout the Term and at all times in connection with its actual or required performance of the contract activities, Contractor will maintain and enforce an information security program that complies with the requirements of the State's data security policies as set forth in the attached **Schedule A** – Data Security Schedule.

(i) Prior to the State procuring Contractor's Products and Services, Contractor will make available to the State with Product-specific and/or Service-specific documentation, including data privacy and/or security sheets. Contractor will comply with all Product-specific and/or Service-specific documentation, and any changes must not result in a material degradation of the overall security of the Services. Moreover, Contractor shall: a) keep Customer Data secure pursuant to the terms of the attached **Schedule A** Data Security Schedule; b) keep such data confidential and only share such data with Hosting Providers approved by the State or third parties engaged by Contractor that are identified in the Contractor's product-specific and/or service-specific documentation ("sub-processors") who must have agreed contractually with Contractor to confidentiality, applicable law and other requirements that are consistent with Contractor's obligations to the State under this Contract.

(b) Third Party Components. Throughout the Term, Contractor will make available updated information identifying and describing any third party and Open-Source Components included in the Contractor's Products and Services.

(c) Data Storage, Backup, Restoration and Disaster Recovery. at all times in connection with its actual or required provision of services as purchased by the State pursuant to this Contract, Contractor will comply with all data storage, backup, restoration, and disaster recovery requirements with respect to its storage, backup, and processing of Customer Data, as set forth in any Contractor websites, portals, ordering documents, or any other representations.

2.6 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.

2.7 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.

2.8 Contractor represents and warrants to the State that:

(a) Contractor must implement tools and measures designed to prevent the introduction of any viruses, worms, spyware, traps, protecting codes, trap door devices, or any other similar devices or mechanisms into the Services that would cause the Services to provide improper access to Customer Data or disclose Customer Data to unauthorized third parties.

(b) Contractor will not advertise through the Cloud Software (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;

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

2.10 Contractor, its subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

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

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

2.13 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 or Federal Court. Court actions against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

2.14 **Accessibility Requirements**.

(a) Contractor will provide a VPAT for the AWS ElasticWolf Client Console and AWS Command Line Interface (CLI). The AWS ElasticWolf Client Console has been assessed for conformance to accessibility standards including the Web Content Accessibility Guidelines 2.0 at the A-AA priority levels. The CLI has been assessed for conformance to accessibility standards, including the Web Content Accessibility Guidelines 2.1 at the A-AA priority levels. Contractor will continue to evaluate the accessibility of the services as well as internal and external accessibility guidance (such as, for example the Web Content Accessibility Guidelines 2.1 Conformance Level AA Success Criteria, as amended and updated over time), and will continue to improve the accessibility of the Services.

(b) AWS will provide Customer with a mechanism for reporting accessibility defects, and will use commercially reasonable efforts to address those defects in accordance with AWS internal processes for prioritization and remediation.

(c) State of Michigan Digital Standards Review. Contractor agrees to cooperate with the State (including the completion State's standards review) should there be any questions about Contractor's ability to meet the standards listed above.

2.15 Insurance. Contractor will maintain the insurance required in the attached **Schedule B**.

3. Additional Terms. Notwithstanding anything to the contrary found on any Contractor websites, portals, ordering documents, or any other representations**,** the parties agree that:

3.1 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.

3.2 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for nor bind the other party in any manner whatsoever.

3.3 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.

3.4 Modification. This Contract may be modified only by a written document executed by the parties hereto.

3.5 **Administrative Fee and Reporting.** Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made online by check or credit card:

State of MI Admin Fees: https://www.thepayplace.com/mi/dtmb/adminfee

State of Mi MiDEAL Fees: https://www.thepayplace.com/mi/dtmb/midealfee

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.

3.6 **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.

(a) 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.

(b) If extended, Contractor must supply all Services and Deliverables 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.

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

3.7 Force Majeure. Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war. No Force Majeure event modifies or excuses Contractor's obligations under Section 2.5 or any disaster recovery, data backup or restoration, data retention, or security requirements under the Contract.

3.8 AWS Service Terms. The AWS Service Terms are incorporated into this Addendum. The Service Terms are the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

SCHEDULE A – Data Security Schedule

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.

"**Customer Data**" or "Customer Content" means Content that Customer or any End User provides to AWS for connecting, processing, storage or hosting by the Services in connection with an AWS Enterprise Account and any computational results that Customer or any End User derive from the foregoing through its use of the Services. For example, Customer Content includes Content that Customer or any End User stores in Amazon Simple Storage Service. Customer Content does not include Account Information

"**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.).

"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.

"**Hosting Provider"** means Contractor and any subprocessor that is providing any or all of the Hosted Services under this Contract.

"Hosted Services" means. each of the services made available by AWS or its Affiliates for which Customer registers via the AWS Site (or by such other means made available by AWS), including those web services described in the Service Terms. Services do not include Third-Party Content.

"**NIST**" means the National Institute of Standards and Technology.

"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).

"**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 facilitate a response to the State's inquiries regarding the security of the Hosted Services including involving Contractor employees who have 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 for the AWS Network, including physical, technical, administrative, and organizational safeguards, that is designed to:

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

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

(c) protect against unauthorized disclosure, access to, or use of the Customer Data;

(d) ensure the complete disposal of any Customer Data as directed by the Customer; and

(e) ensure that all Contractor employees and subcontractors 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 for the Contractor's FedRAMP authorized products and/or services, be less stringent than the safeguards of the FedRAMP requirements and any other compliance standards identified as met at the initial use of the service by the State.

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

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

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

5.1 For those Hosted Services that are identified by Contractor as FedRAMP authorized, Contactor will maintain FedRAMP authorization throughout the term. In the event Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may immediately terminate those services under this Contract, or any portion thereof, for termination for the public interest, regardless of any minimum commitment made with the understanding that the services would remain FedRAMP authorized, and such termination will be without cost to the State, including the waiver of any early termination fees.;

5.2 for Contractor's products and/or services identified as FedRAMP authorized, 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. In the event Hosting Provider is unable to maintain the authorizations of this Section 5.2, the State, at its sole discretion, may immediately terminate those services under this Contract, or any portion thereof, for termination for the public interest, regardless of any minimum commitment made with the understanding that the services would retain and provide either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II, and such termination will be without cost to the State, including the waiver of any early termination fees.;

5.3 for Contractor's products and/or services identified as FedRAMP authorized, if the Customer selects AWS Services identified in applicable Documentation as FedRAMP compliant, then Contractor or its Services will only host, store, support, access, administer, back up, and process Customer Data in data center(s) that reside in the continental United States and in accordance and consistent with the Services' FedRAMP authorization impact level;

5.4 for Contractor's FedRAMP authorized products and/or services, maintain and enforce an information security program including safety and physical and technical security policies and procedures designed to provide at least the same level of protection as evidenced by its FedRAMP or Security Reference Guide ("SRG") ATOs (or its equivalent, as mutually agreed upon), on the Effective Date;

5.5 maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the Customer Data that complies with the representations identified in the Contractor's product-specific and/or service-specific documentation at the time use of product or services was first initiated;

5.6 for Contractor's FedRAMP authorized products and/or services, 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 Customer Data and the nature of such Customer 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 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 Customer Data and the nature of such Customer Data, consistent with best industry practice and the Contractor's product-specific and/or service-specific documentation at the time use of product or services was first initiated;

5.8 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) Customer 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 Customer Data;

5.9 ensure that Customer Data can be encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

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

5.11 for products and/or services identified as HIPAA compliant, 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

5.12 for data deleted by the State and for Contractor's product and/or services no longer used by the state, Contractor must permanently sanitize or destroy Customer 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 sanitation methods or otherwise in accordance with the Contractor's product-specific and/or service-specific documentation, including timeframes.

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

6. Security Accreditation Process. Throughout the Term, Contractor will provide reasonable cooperation to assist the State to obtain and maintain its authority to operate (ATO), including, but not limited to, providing the State with Contractor's system security plan (SSP) upon 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). Consistent with Contractor's product-specific and/or service-specific documentation safeguards, all identified risks from the SSP will be remediated based on the risk level of the identified risk. 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.' Contractor documentation provided under this Section to the State will be treated as Contractor's Confidential Information.

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 With respect to the AWS Network, and during the Term, Contractor (including Chain Subcontractors) will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to Customer Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the Customer 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 will have access to third party attestations in AWS Artifact (or any subsequent iteration) through the Contract Term. The State may, but is not obligated to, perform penetration tests in accordance with Contractor's Penetration Testing Policy (available at http://aws.amazon.com/security/penetration-testing/ or any successor or related locations designated by Contractor).

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 as soon as the plan(s) or report(s) are available within AWS Artifact, or within two weeks of the State's request. Reports will be recognized as Contractor's Confidential Information.

8.4 During the Term, AWS will maintain an information security program designed to provide at least the same level of protection necessary to maintain FedRAMP compliance in place on the Effective Date. If exceptions are identified in any SOC Report (or its equivalent), AWS will take reasonable steps to remediate those exceptions.

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 in compliance with applicable legal and regulatory requirements as identified Contractor's product-specific and/or service-specific documentation

Contractor's application scanning and remediation must include each of the following types of scans and activities or materially equivalent industry practices:

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

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

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

(a) 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 in the Contractor's product-specific and/or service-specific documentation 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 in scope as of the Effective Date, Contractor must ensure the Contractors infrastructure and applications are scanned using a PCI Approved Vulnerability Scanning Tool at least quarterly and other vulnerability scanning tools on a regular basis, but in any event no less than monthly; and make available to the State, verification of the scans and appropriate vulnerability remediation.

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 Customer 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 A, Attachment 1 – Tax Regulation, PCI Compliance, CEPAS, and CJIS, etc.…

SCHEDULE B – Insurance Schedule

Required Coverage.

1. Insurance Requirements. Contractor, at its sole expense, must maintain the insurance coverage identified below for the term of the Contract. Contractor can satisfy the foregoing minimum limits by any combination of primary liability, umbrella excess liability, and self-insurance coverage that results in the same protection. All required insurance must (i) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State and other than for Contractor coverage by self-insurance and (iii) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

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	Policy must be 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 2010 07 04 and CG 2037 07 04.
Workers' Compensation Insurance	
Minimum Limits: Coverage according to statutory limits as required by applicable U.S. 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 $2,000,000 Annual Aggregate	Policy must cover information security and privacy liability, privacy notification costs, and regulatory defense and penalties.

1. If any required policies provide claims-made coverage, the Contractor must: (i) provide coverage with a retroactive date before the Effective Date of the Contract or the beginning of Contract; (ii) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract; and (iii) 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, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

2. Contractor must: (i) provide a memorandum of insurance for proof of self-insured coverage or insurance certificates for commercial policies to the Contract Administrator, at Contract formation; and (ii) (iv) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

3. This Section is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

SCHEDULE C - Federal Provisions Addendum

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

1. Equal Employment Opportunity

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

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

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

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

(3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

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

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

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

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

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

> Provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.
>
> The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: *Provided,* that if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.
>
> The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.
>
> The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

2. Davis-Bacon Act (Prevailing Wage)

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

(1) All transactions regarding this contract shall be done in compliance with the Davis-Bacon Act (40 U.S.C. 3141- 3144, and 3146-3148) and the requirements of 29 C.F.R. pt. 5 as may be applicable. The contractor shall comply with 40 U.S.C. 3141-3144, and 3146-3148 and the requirements of 29 C.F.R. pt. 5 as applicable.

(2) Contractors are required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.

(3) Additionally, contractors are required to pay wages not less than once a week.

3. Copeland "Anti-Kickback" Act

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

(1) Contractor. The Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into this contract.

(2) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clause above and such other clauses as FEMA or the applicable federal awarding agency may by appropriate instructions require, and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses.

(3) Breach. A breach of the contract clauses above may be grounds for termination of the contract, and for debarment as a Contractor and Subcontractor as provided in 29 C.F.R. § 5.12.

4. Contract Work Hours and Safety Standards Act

If the Contract is **in excess of $100,000** and **involves the employment of mechanics or laborers**, the Contractor must comply with 40 USC 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5), as applicable, and during performance of this Contract the Contractor agrees as follows:

(1) Overtime requirements. No Contractor or Subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

(2) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (1) of this section the Contractor and any Subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such Contractor and Subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (1) of this section, in the sum of $27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (1) of this section.

(3) Withholding for unpaid wages and liquidated damages. The State shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold

or cause to be withheld, from any moneys payable on account of work performed by the Contractor or Subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (2) of this section.

(4) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clauses set forth in paragraph (1) through (4) of this section and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (1) through (4) of this section.

5. Rights to Inventions Made Under a Contract or Agreement

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

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

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

Clean Air Act

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

Federal Water Pollution Control Act

(1) The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

(2) As required by the Federal Water Pollution Control Act, the Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.

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

7. Debarment and Suspension

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

(1) This Contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, the Contractor is required to verify that none of the Contractor's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(2) The Contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(3) This certification is a material representation of fact relied upon by the State. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the State, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

(4) The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

8. Byrd Anti-Lobbying Amendment

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

9. Procurement of Recovered Materials

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

(1) In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired—

a. Competitively within a timeframe providing for compliance with the contract performance schedule;

b. Meeting contract performance requirements; or

c. At a reasonable price.

(2) Information about this requirement, along with the list of EPA- designated items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensive- procurement-guideline-cpg-program.

(3) The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

10. Additional FEMA Contract Provisions.

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

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

a. The Contractor agrees to provide the State, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.

b. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

c. The Contractor agrees to provide the FEMA Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the contract.

d. In compliance with the Disaster Recovery Act of 2018, the State and the Contractor acknowledge and agree that no language in this contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

(2) Changes.

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

(3) DHS Seal, Logo, And Flags.

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

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

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

(5) No Obligation by Federal Government.

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

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

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

Schedule H, Attachment 1 - Byrd Anti-Lobbying Certification

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

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

Certification for Contracts, Grants, Loans, and Cooperative Agreements

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

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

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

____
Signature of Contractor’s Authorized Official

____
Name and Title of Contractor’s Authorized Official

____
Date