

Contract no. MCSA0080

AWS Enterprise Agreement

This AWS Enterprise Agreement (this "Agreement") is made and entered into by and between Amazon Web Services, Inc., a Delaware corporation ("AWS") and the customer specified on this Cover Page ("Customer" or the "State").

In consideration of the mutual promises contained in this Agreement, AWS and Customer agree to all terms of the Agreement effective as of the date the last party signs this Agreement (the "Effective Date").

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

<p>Amazon Web Services, Inc.</p> <p>By: <u>[Signature]</u></p> <p>Name: <u>Shahin Lawther</u></p> <p>Title: <u>Authorized Representative</u></p> <p>Signature Date: <u>10/30/18</u></p> <p>Address:</p> <p>410 Terry Avenue North Seattle, WA 98109-5210 Attention: AWS General Counsel Fax: 206-266-7010</p>	<p>Customer Name: State of Ohio Department of Administrative Services</p> <p>By: <u>[Signature]</u></p> <p>Name: <u>Robert Blair</u></p> <p>Title: <u>Director</u></p> <p>Signature Date: <u>10.31.18</u></p> <p>Address:</p> <p>State of Ohio Department of Administrative Services Office of the Chief Legal Counsel 30 East Broad Street, 40<sup>th</sup> Floor Columbus, Ohio 43215 Attention: Christine M. Kinworthy, Associate Counsel Fax:</p>
---	---



## 1. Use of the Service Offerings.

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

**1.2 AWS Account.** To access the Services, Customer must create one or more AWS Enterprise Accounts. Unless explicitly permitted by the Service Terms, Customer will only create one AWS Enterprise Account per email address. All AWS Enterprise Accounts will be covered by this Agreement. For all AWS Enterprise Accounts, this Agreement 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 AWS accounts do not meet the definition of an "AWS 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 Agreement 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, or by issuing a purchase order to AWS in accordance with Section 14(h). Customer may open accounts on behalf of State Entities and in such event, State Entities will be End Users of Customer under the Agreement. In addition, any Customer Affiliate may purchase AWS Services as described below in this Section 1.4.

(a) For Customer to open an AWS Enterprise Account for use by a State Entity, such AWS account must: (a) be opened by the Customer using an email address issued by the State Entity or the Customer (with an email domain name that is owned by the State Entity or the Customer); (b) be joined in an Organization for which Customer's AWS account number is identified to AWS by Customer in writing as the Master Account for purposes of AWS Organizations (or any successor Service offered by AWS); and (c) include the State Entity's full legal name in the "Company Name" field associated with the AWS account.

(b) For those Customer Affiliates that are Cooperative Purchasing Members who elect to procure AWS Services subject to the terms of this Agreement, such Cooperative Purchasing Member's access and use of the Service Offerings will be governed by this Agreement and the terms of this Agreement will be read to apply to the Cooperative Purchasing Member as the Customer of AWS except that AWS will have no reporting or cost recovery fee obligations to any Cooperative Purchasing Member. Each Cooperative Purchasing Member is solely responsible and liable for any actions that occur from it or its End User's use of the AWS Services and all activities under its accounts. Nothing in this Agreement requires AWS to accept a purchase order from a Cooperative Purchasing Member.

(c) For those Customer Affiliates that are Non Superintended Entities who elect to procure AWS Services subject to the terms of this Agreement, such entity's access and use of the Service Offerings will be governed by this Agreement and the terms of this Agreement will be read to apply to the Non Superintended Entity as the Customer of AWS except that AWS will have no reporting or cost recovery fee obligations to any Non Superintended Entities (but will report any purchases made by such entities to Customer in accordance with Section 14(h) of this Agreement). Each Non Superintended Entity is solely responsible and liable for any actions that occur from it or its End User's use of the AWS Services and all activities under its accounts. Nothing in this Agreement requires AWS to accept a purchase order from a Non Superintended Entity.

(d) If at any time during the Term a Customer Affiliate no longer meets the definition of an "Affiliate" of Customer, then (i) it will no longer be an Affiliate for purposes of this Agreement, and (ii) that former Customer Affiliate and its AWS accounts will no longer be covered under this Agreement (and in the absence of any other agreement between the former Customer Affiliate and AWS, all AWS accounts of such former Affiliate will be governed by the AWS Customer Agreement).

**1.5 Customer Reports.** AWS shall be responsible for reporting all revenue from the Services purchased under this Agreement. AWS will submit quarterly reports to Customer via the Customer's designated website and in accordance with the process identified in Section 14 of the Agreement. AWS will submit all reports and the quarterly Cost Recovery Fee owed to the State by the 15<sup>th</sup> day of the month following the month after the State's fiscal quarter ends. The State fiscal quarters run as follows: quarter 1 is July 1<sup>st</sup> to September 30<sup>th</sup>, quarter 2 is October 1<sup>st</sup> to December 31<sup>st</sup>, quarter 3 is January 1<sup>st</sup> through March 31<sup>st</sup>, and quarter 4 is April 1<sup>st</sup> through June 30<sup>th</sup>. In the event the 15<sup>th</sup> day of the month after a fiscal quarter falls on a state or federal holiday or weekend then the Cost Recovery Fee payment and quarterly report will not be due to the State until the first business day following the 15<sup>th</sup>. In addition, AWS must provide the State with a recap of the services provided to Cooperative Purchasing Members on a quarterly basis in a form substantially similar to the report attached as Exhibit 2 (such reports may be submitted via email to Dennis Kapenga at [dennis.kapenga@das.ohio.gov](mailto:dennis.kapenga@das.ohio.gov), or such other contact person and email address as the State may update from time to time upon email notice to AWS).

In addition, to assist the State with generating monthly reports regarding the State's use of AWS Service, the State may use the AWS Management Console so the State of Ohio, Office of Information Technology, may generate monthly reports providing such reasonable information regarding Services purchased and fees charged under this Agreement as the State of Ohio, Office of Information Technology requests to permit accurate tracking and monitoring of its activity under this Agreement.

## 2. Changes.

**2.1 To the Service Offerings.** AWS may change or discontinue any of the Service Offerings, from time to time. For any AWS 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.

**2.3 To the APIs.** AWS may change or discontinue any APIs for the Services from time to time. For any change or discontinuation of an API that is not also a discontinuation of a Service or a functionality of a Service, AWS will continue supporting the previous version of such API for 12 months after the change or discontinuation (except if doing so (a) would pose a security or intellectual property issue, (b) is technically infeasible, or (c) is needed to comply with the law or requests of governmental entities).

## 3. Privacy and Security.

**3.1 AWS Security.** AWS will implement reasonable and appropriate measures for the AWS Network (as determined by AWS) designed to help Customer secure Customer Content against accidental or unlawful loss, access or disclosure (the "Security Objectives") in accordance with the AWS Security Standards. AWS may modify the AWS Security Standards from time to time, but will continue to provide at least the same level of security as is described in the AWS 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. AWS will only use Account Information in accordance with the Privacy Policy, and Customer consents to such usage. The Privacy Policy 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 Agreement, AWS may process Service Attributes where AWS maintains its support and investigation personnel.

**3.4 AWS Information Security Program.** As of the Effective Date, AWS is certified under ISO 27001. AWS will maintain an information security program designed to provide at least the same level of protection as evidenced by its certification under ISO 27001 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 its Service 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 provide this documentation no more than twice annually and this documentation will be treated as Confidential Information of AWS under the NDA.

#### 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 AWS Enterprise Accounts and Customer Content, such as, for example, using enhanced access controls to prevent unauthorized access to AWS 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 Agreement, as between the parties, Customer is responsible for all activities that occur under its AWS 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 Agreement and that any terms of any agreement with each End User are not inconsistent with this Agreement. 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 AWS 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 AWS 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. If the parties fail to resolve the dispute within such 30 day period, AWS may, at its



option, (a) suspend Customer's or any End User's right to access or use any portion or all of the Service Offerings, immediately upon notice to Customer, and (b) terminate this Agreement pursuant to Section 7.2(b). All amounts payable by Customer under this Agreement 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 AWS 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 advance Notice. AWS may elect to charge Customer interest on all late payments to the extent permitted by Section 126.30 ("Prompt Payment Requirements") of the Ohio Revised Code.

**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 Agreement. All fees payable by Customer are exclusive of Indirect Taxes. 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 Agreement 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 Agreement. 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 Agreement.

**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 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 Agreement will commence on the Effective Date and will remain in effect until terminated pursuant to this Agreement. Any Notice of termination of this Agreement by either party to the other must include a Termination Date. The Parties acknowledge that Customer may immediately terminate this Agreement under section 7.2(a) ("Termination for Convenience") in order to comply with any applicable appropriation or contract funding rules and requirements.

### **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 Either Party.** Either party may terminate this Agreement for cause if the other party 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 other 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 Section 7.3(b), all of Customer's rights under this Agreement 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 AWS, destroy all AWS Content in Customer's possession (except for AWS Content that is publicly available on the AWS Site); and
- (iv) Sections 4, 5, 7.3, 8.1, 8.3, 8.4, 9, 10.3, 11, 12 and 13 will continue to apply 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 AWS, Customer (or Customer's licensors) own all right, title, and interest in and to Customer Content. Except as provided in this Agreement, AWS obtains no rights under this Agreement from Customer (or Customer's licensors) to Customer Content.

**8.2 Service Offerings License.** AWS 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, AWS 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 AWS 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 AWS 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 AWS Content. AWS agrees that, at no cost to the State, AWS will permit the transfer of this Agreement to a resulting agency in the event the State merges or consolidates State entities and the administration of this Agreement is delegated to another agency. AWS and the State will work together to effect the transfer.

**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 AWS Marks in accordance with the Trademark Use Guidelines. Customer will not misrepresent or embellish the relationship between AWS and Customer (including by expressing or implying that AWS supports,



sponsors, endorses, or contributes to Customer or Customer's business endeavors). Customer will not imply any relationship or affiliation between AWS and Customer except as expressly permitted by this Agreement.

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

**9. Third-Party Claims. 9.1 Customer Representations, Warranties, and Covenants.** Customer represents, warrants, and covenants that (i) Customer and any End Users' use of the Service Offerings (including any activities under an AWS Enterprise Account and use by Customer's employees and personnel) and Customer Content will not violate this Agreement or applicable law; (ii) Customer Content, the combination of Customer Content with other applications, content or processes, or the use, development, design, production, advertising, or marketing of Customer Content, do not and will not infringe or misappropriate any third-party rights; and (iii) Customer's use of the Service Offerings will not cause harm to any End Users.

**9.2 Intellectual Property.**

(a) Subject to the limitations in this Section 9, if Customer obtains and provides AWS with written consent from the Ohio Attorney General, 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 AWS will pay the amount of any adverse final judgment or settlement.

(b) [RESERVED].

(c) AWS will have obligations and liability under this Section 9.2 only to the extent caused by the infringement of an unaffiliated third party's intellectual property rights by the Services (i.e., no obligations or liability for infringement by combinations of the Services with any other product, service, software, data, content, or method not supplied by AWS, including any Third-Party Content or Customer Content, to the extent that the Services would not infringe but for such combination). 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 Agreement.

**9.3 Process.** AWS's obligations under this Section 9 will apply only if: (a) Customer gives AWS prompt written notice of the claim; (b) Customer and the Ohio Attorney General permit AWS to control the defense and settlement of the claim; and (c) Customer and the Ohio Attorney General reasonably cooperate with AWS (at AWS' expense) in the defense and settlement of the claim. While AWS may settle any claim on behalf of AWS, its Affiliates, and their respective employees, officers, directors, and representatives, in no event will AWS agree to any settlement of any claim on behalf of Customer without the written consent of Customer and the Ohio Attorney General.**10. AWS Warranties and Warranty Disclaimers.**

**10.1 AWS Warranties.** AWS represents and warrants to Customer that: (a) the Services will perform substantially in accordance with the Documentation, and (b) it will use commercially reasonable efforts to ensure that those portions of the Services that are of a type ordinarily affected by viruses utilize enterprise-grade security software designed to detect and remove malicious or hidden mechanisms or code designed to damage or corrupt the Services or Customer Content.

**10.2 Mutual Warranties.** Each party 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, AWS, 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 CUSTOMER OBLIGATIONS ARISING UNDER SECTION 9.1, NEITHER PARTY NOR ANY OF THEIR AFFILIATES OR LICENSORS WILL BE LIABLE TO THE OTHER PARTY 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 CUSTOMER OBLIGATIONS AND AWS PAYMENT OBLIGATIONS ARISING UNDER SECTION 9, THE AGGREGATE LIABILITY UNDER THIS AGREEMENT OF EITHER PARTY AND ANY OF THEIR RESPECTIVE AFFILIATES OR LICENSORS WILL NOT EXCEED THE LESSER OF (A) 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, OR (B) USD \$20,000,000; 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.

## **12. Miscellaneous.**

**12.1 Assignment.** Neither party 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 party; except that either party may assign or otherwise transfer this Agreement without the consent of the other party (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. 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. In the event of an Assignment under this section the assignee will provide notice of the Assignment after the Assignment occurs and will be delivered within a reasonable time, as determined by the assignee, to the non-assigning party. The notice provide by the assignee may be in whatever form is reasonable under the circumstances.

**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.**

(a) This Agreement incorporates the Policies and any amendments or addenda to this Agreement ("**Addenda**") by reference and is the entire agreement between Customer and AWS regarding the subject matter of this Agreement. This Agreement supersedes all prior or contemporaneous representations, understandings, agreements, or communications between Customer and AWS, whether written or verbal, regarding the subject matter of this Agreement (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 Agreement (whether or not it would materially alter this Agreement) including for example, any term, condition or other provision (a) submitted by Customer in any order, receipt, acceptance, confirmation, correspondence or other document, (b) related to any online registration, response to any Request for Bid, Request for Proposal, Request for Information, or other



questionnaire, or (c) related to any invoicing process that Customer submits or requires AWS to complete. If the terms within the body of this document or Attachment A are inconsistent with the terms contained in any Policies, the terms contained within the body of this document and Attachment A will control, except that the Service Terms will control over the body of this document and Attachment A. No modification or amendment of any portion of this Agreement will be effective unless in writing and signed by the parties to this Agreement.

(b) The portion of any provision in the Policies or the Addenda on or after the Effective Date that purports to bind the parties to a particular governing law, venue, arbitration procedure or alternative dispute resolution process ("**Dispute Provisions**") will not be binding on the parties to the extent such Dispute Provisions conflict with applicable Ohio state law. Also, the portion of any provision in the Policies or Addenda that requires Customer to indemnify AWS ("**Indemnification Provisions**") shall not be construed as an indemnification obligation by Customer; rather, such portion of such Indemnification Provisions shall be read as a representation and warranty by Customer that the harm to which the indemnification obligation relates will not occur. The manner in which the parties have amended Section 9.1 of this Agreement illustrates the foregoing construction and provides a non-limiting example of how other Indemnification Provisions shall be construed, as does the following: The last sentence of Section 6.7 of the Service Terms, which states: "You will indemnify and reimburse Amazon Payments and its affiliates against any claim or demand for payment of any such taxes or any Chargebacks" shall be construed to mean: "You represent and warrant that your use of the Services will not give rise to any claim or demand for payment of any such taxes or Chargebacks made against Amazon Payments and its affiliates." The parties agree this construction of any Indemnification Provision shall render a breach of such representation and warranty actionable as a breach of warranty and breach of contract, not as an indemnification obligation by Customer. For clarity, the above limitations regarding Dispute Provisions and Indemnification Provisions shall apply regardless of any current or future language in the Policies or Addenda purporting to apply and govern over the Agreement, regardless of what is stated in the Policies or Addenda.

**12.4 Force Majeure.** Neither party will be liable for any delay or failure to perform any obligation under this Agreement 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 Governing Law; Venue.** The laws of the State of Ohio, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between the parties. Any dispute relating in any way to the Service Offerings or this Agreement will only be adjudicated in a state or federal court located in Franklin County, Ohio. Each party consents to exclusive jurisdiction and venue in these courts. Notwithstanding the foregoing, either party may seek injunctive relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of such party's, its Affiliates' or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

**12.6 Trade Compliance.** In connection with this Agreement, 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 or an instrumentality of the State of Ohio, as applicable, 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. Each party represents that it is 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 party, or 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 Agreement must be in the English language. If AWS provides a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

**12.9 Nondisclosure; Publicity.** The parties' NDA is hereby incorporated into this Agreement, except that the security provisions in Section 3, not the NDA, apply to Customer Content. Neither party will issue any press release or make any other public communication with respect to this Agreement or Customer's use of the Service Offerings unless otherwise provided in the Agreement. Customer may disclose Confidential Information only as required by the Ohio Revised Code ("ORC") Section 149.43 to comply with public records requests and orders of governmental entities with jurisdiction over it, if Customer, when possible and in accordance with ORC Section 149.43 (i) gives AWS prior written notice sufficient to allow AWS to seek a protective order or other remedy (except to the extent that Customer's compliance would cause it to violate an order of the governmental entity, Ohio law, or other legal requirement), (ii) discloses only such information as is required, and (iii) uses commercially reasonable efforts to obtain confidential treatment for any Confidential Information so disclosed. Regardless of any other term in this Agreement, release of public records in compliance with Ohio law will not be deemed a breach of the Agreement.

**12.10 Notice.**

**(a) General.** Except as otherwise set forth in Section 12.10(b), to give notice to a party under this Agreement, each party must contact the 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 Agreement or addressed to the address of the other party listed on the Cover Page to this Agreement, or such other fax number or address as a party may subsequently provide in writing to the other party. 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 either party to enforce any provision of this Agreement 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.

**12.14 Insurance.** During the Term, AWS will obtain and maintain the following: (a) 'Commercial General Liability' insurance with limits of not less than \$1,000,000 per occurrence and \$2,000,000 general aggregate, and (b) 'Errors and Omissions' insurance with limits of not less than \$1,000,000 per claim.

**13. Definitions.** Defined terms used in this Agreement 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: (i) as to AWS, any entity that directly or indirectly controls AWS, is controlled by AWS, or is under common control with AWS; and (ii) as to Customer, those entities identified on Exhibit 1 as State Entities, Non Superintended Entities, or any Cooperative Purchasing Member.

**"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 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), and (c) includes Customer's full legal name in the "Company Name" field associated with the AWS account.

**"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) 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 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.

**"Cooperative Purchasing Member"** or **"Co-op Member"** means any entity that has qualified for participation in the State of Ohio's cooperative purchasing program under Section 125.04 of the Ohio Revised Code that is not otherwise identified as one of the State Entities on Exhibit 1.

**"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.

**"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).

**"NDA"** means the Unilateral Nondisclosure Agreement entered into between Amazon.com, Inc. the State of Ohio, DAS OIT.

**"Non Superintended Entity" or "Non Superintended Entities"** means those entities identified on Exhibit 1 under the Title, "Non Superintended Legislative, Judicial, and Elected Entities".

**"Notice"** means any notice provided in accordance with Section 12.10.

**"Policies"** means the Acceptable Use Policy, Privacy Policy, and the Service Terms.

**"Privacy Policy"** means the privacy policy 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.

**"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. For the avoidance of doubt, Service Offerings include the services offered in the AWS GovCloud(US) region.

**"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.

**"State Entity" or "State Entities"** means those entities identified on Exhibit 1 as Cabinet Level Superintended State Agencies and Other Superintended State Agencies which the State may update from time to time by emailing an updated list to AWS at [aws-wwps-ohio@amazon.com](mailto:aws-wwps-ohio@amazon.com).

**"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 accordance with Section 7, in a Notice from one party to the other.

**"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.

**14. Ohio Master Service Contract Provisions.** The following terms are incorporated into this Agreement.

- (a) **Contract – Renewal.** The State may renew this Agreement in the next biennium by issuing written notice to AWS of the decision to do so. Renewals will be initiated by the State in writing at least 30 days before the expiration of the then current term, if any. This expiration and renewal procedure will also apply to the end of any subsequent biennium. Any Cooperative Purchasing Members receiving Services under this Agreement after an expiration date will continue to receive Services under the terms of the AWS Customer Agreement, available at [aws.amazon.com/agreement](http://aws.amazon.com/agreement) or other agreement between the Cooperative Purchasing Member and AWS.

- (b) **Relationship of the Parties and Cooperative Purchasing Members.** AWS is an independent contractor and is not an agent, servant, or employee of the State.

(c) **Third-Party Suppliers.**

AWS's use of other suppliers to provide the Services under this Agreement does not mean that the State will pay for them. AWS will be solely responsible for payment of its suppliers and any claims of those suppliers for any failure of AWS to meet its obligations under this Agreement in providing the Services in the required manner.

AWS assumes responsibility for all Services provided under this Contract whether it or one of its suppliers provides them in whole or in part. Further, other than Third-Party Content, AWS will be the sole point of contact with regard to contractual matters governing the Services, including payment of all charges resulting from the Agreement for Services.

- (d) **Non-Exclusivity.** This Agreement is non-exclusive and is not a requirements contract. Nothing herein prevents either party from entering into similar agreements with other entities.
- (e) **Competitive Pricing and Services.** As provided in the Agreement, pricing under this Agreement is provided in accordance with the publicly available pricing on the AWS Site. This represents the commercially available pricing for all customers.
- (f) **Public Records Requests.** In accordance with Section 3.2, if AWS receives a public records request for Customer Content, AWS will not (a) disclose Customer Content to any government or third party, except as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order) and 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, to enable Customer to seek a protective order or other appropriate remedy.

**State Reporting Requirements.**

- (g) **Cost Recovery.** AWS must pay a fee to the State to cover the estimated costs the State will incur administering this Agreement and the Services offered under it ("Cost Recovery Fee").

The Cost Recovery Fee will be 2% of the total dollar amount of Services AWS invoices under this Contract to all Cooperative Purchasing Members, including all State-level entities. The Cost Recovery Fee is included in the prices reflected in purchase orders and AWS may not add a surcharge to orders under this Agreement to cover the amount of the Cost Recovery Fee. The State may compare the quarterly revenue reports provided by AWS to information in the State's accounting system, the State's Ordering System, and other records for purposes of verifying the accuracy of the information. AWS will be responsible for paying the quarterly Cost Recovery Fee based on the AWS quarterly reported revenue in accordance with section 1.5 of the Agreement.

- (h) **Purchasing by State Agencies and Cooperative Purchasing Members.** In order for a State Entity, Non Superintendent Entity, or Cooperative Purchasing Member to purchase AWS Services under this Agreement it must issue a purchase order ("PO") to AWS and such PO must set forth the PO number, purchasing party's AWS Account Number, and the Contract number associated with this agreement MCSA0080. Any additional terms set forth on a PO must be agreed upon in signed writing by AWS and the Customer issuing the PO.

Examples of the calculation of a Cost Recovery Fee:

1. An example of a contractor with sales only to State Entities and thus no revenue from Cooperative Purchasing Members:

State Fiscal Year 2015				
Quarter	Total Quarterly Sales from State Entities	Total Quarterly Sales from Co-op Members	Total Revenue Share Due	Reported by
Q1	\$ 79,193	\$ 0	\$ 1,584	Name of Contact
Q2	\$ 10,392	\$ 0	\$ 208	Name of Contact
Q3	\$ 209,105	\$ 0	\$ 4,182	Name of Contact
Q4	\$ 74,970	\$ 0	\$ 1,499	Name of Contact

2. An example of a contractor with sales to both State Entities and Co-op Members and thus revenue from both:

State Fiscal Year 2015				
Quarter	Total Quarterly Sales from State Entities	Total Quarterly Sales from Co-op Members	Total Revenue Share Due	Reported by
Q1	\$ 79,193	\$ 20,963	\$ 2,003	Name of Contact
Q2	\$ 10,392	\$ 4,197	\$ 292	Name of Contact
Q3	\$ 209,105	\$ 63,210	\$ 5,446	Name of Contact
Q4	\$ 74,970	\$ 1,471	\$ 1,529	Name of Contact

3. An example of a contractor with sales to neither State Entities nor Co-op Members and thus no revenue to report:

State Fiscal Year 2015				
Quarter	Total Quarterly Sales from State Entities	Total Quarterly Sales from Co-op Members	Total Revenue Share Due	Reported by
Q1	\$0	\$0	\$0	Name of Contact
Q2	\$0	\$0	\$0	Name of Contact
Q3	\$0	\$0	\$0	Name of Contact
Q4	\$0	\$0	\$0	Name of Contact

AWS must use the State’s Web-based system for reporting revenue generated under this Contract. Upon execution of this Agreement, the State will promptly send AWS the web-link needed for AWS to access and submit the reports required under this Agreement.

AWS must remit the 2% Cost Recovery Fee to the State quarterly by check to the State of Ohio, Office of Information Technology. The check must be made payable to the Treasurer, State of Ohio, and must be sent to the State at the following address:

Department of Administrative Services  
 L-3686  
 Columbus, OH 43260-3686



To ensure that the payment is credited properly, AWS must identify the payment as a State of Ohio Cost Recovery Fee and reference this Agreement. Credit for the Cost Recovery Fee will begin in the month of execution of this Agreement.

The first payment will be calculated against all Services rendered to the existing Cooperative Purchasing Members transferred to the Agreement in the month of effective date, if any as of the date such Cooperative Purchasing Member transferred to the Agreement. Subsequent payments will be calculated against all Cooperative Purchasing Members as stated above.

The Contractor's contact person for Cost Recovery Section will be:

Name: John Malloy  
 Address: 410 Terry Ave., North, Seattle, WA 98109  
 Phone: 202-629-4169  
 Email: jmmall@amazon.com  
 Email for reporting notifications: aws-wwps-ohio@amazon.com

- (i) **Employment Taxes.** Each party will be solely responsible for reporting, withholding, and paying all employment related taxes, contributions, and withholdings for its own personnel, including, but not limited to, federal, state, and local income taxes, and social security, unemployment and disability deductions, withholdings, and contributions, together with any interest and penalties.
- (j) **Equal Employment Opportunity.** AWS will comply with all applicable state and federal laws regarding equal employment opportunity and fair labor and employment practices, including ORC Section 125.111 and all related Executive Orders.

Before this Contract can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the DAS Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by to the Ohio Business Gateway at:

<http://business.ohio.gov/efiling/>

The State encourages the Contractor to purchase goods and services from Minority Business Enterprises ("MBEs") and Encouraging Diversity, Growth and Equity ("EDGE") contractors

- (k) **Drug-Free Workplace.** The Contractor must comply with all applicable state and federal laws regarding keeping a drug-free workplace. The Contractor must make a good faith effort to ensure that all its employees, while working on State property or the property of any Subscriber, will not have or be under the influence of illegal drugs or alcohol or abuse prescription drugs in any way.
- (l) **Conflicts of Interest.** No Contractor personnel may voluntarily acquire any personal interest that conflicts with the Contractor's responsibilities under this Contract. Additionally, the Contractor will not knowingly permit any public official or public employee who has any responsibilities related to this Contract to acquire an interest in anything or any entity under the Contractor's control, if such an interest would conflict with that official's or employee's duties. The Contractor will disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Contract. The Contractor will take all reasonable legal steps to ensure that such a person does not participate in any action affecting the work under this Contract, unless the State has determined that, in the light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.



- (m) **Findings for Recovery.** The Contractor warrants that the Contractor is not subject to an unresolved finding for recovery under ORC §9.24. If the warranty is false on the date the Parties signed this Contract, the Contract is void *ab initio*.
- (n) **Anti-Trust.** The Parties recognize that, in actual economic practice, overcharges resulting from antitrust violations are usually borne by the State and the Subscribers. The Contractor therefore assigns to the State all state and federal antitrust claims and causes of action that the Contractor now has or may acquire relating to the Services that are covered by this Contract.
- (o) **Campaign Contributions.** By signing this document, the Contractor certifies that all applicable parties listed in ORC Section 3517.13 are in full compliance with ORC Section 3517.13.
- (p) **Safety and Security Rules.** When on any property owned or controlled by the State, the Contractor must comply with all security and safety rules in Attachment C that are expressly required of the Contractor or which the Contractor is required to apply to people on those premises as communicated by the State in the applicable scope of work. Cooperative Purchasing Members may have policies and regulations that are specific to them and with which the Contractor must also comply prior to conducting work on the Cooperative Purchasing Members' premises.
- (q) **Ohio Ethics Law.** The Contractor certifies that it is currently in compliance with and will continue to adhere to the applicable requirements of the Ohio ethics laws. The Contractor also certifies that all applicable parties listed in Ohio Revised Code Section 3517.13 are in full compliance with that section.
- (r) **Survival.** Any terms or conditions contained in this Agreement that must survive termination of this Agreement to be fully effective will survive the termination of the Agreement, unless expressly provided otherwise in this Agreement. Additionally, no termination of the Contract will affect the State's right to receive Services for which the State has paid before termination. If any Agreement with a Cooperative Purchasing Member should expire or be terminated, the remaining portions of this Contract will survive.
- (s) **No Waiver.** The failure of a Party to demand strict performance of any terms or conditions of this Agreement may not be construed as a waiver of those terms or conditions, and that Party may later demand strict and complete performance by the other Party.
- (t) **Headings.** The headings herein are for convenience only and are not intended to have any substantive significance in interpreting this Agreement.
- (u) **Travel Expenses.** Any travel that the Contractor requires to perform its obligations under this Agreement will be at the Contractor's expense. The State will pay for any additional travel that it requests only with prior written approval. The State will pay for all additional travel expenses that it requests in accordance with the State's travel policy in Rule126-1-02 of the Ohio Administrative Code.



## Attachment B AWS Security Standards

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

## Attachment C – State IT Security Standards and Policies

### 1. Overview and Scope

This Attachment C to the AWS Enterprise Agreement entered into by and between AWS and the State (this "Attachment") shall apply to any and all Services that AWS provides to the State under the AWS Enterprise Agreement and access to State resources provided in conjunction with delivery of the Services.

The terms in this Attachment are additive to the terms and conditions of the AWS Enterprise Agreement. In the event of a conflict between the terms of the AWS Enterprise Agreement and this Attachment, the AWS Enterprise Agreement shall prevail. The AWS Enterprise Agreement and this Attachment together form "the Agreement" for purposes of the terms contained herein. For purposes of this Attachment references to "Contractor" means AWS and references to the "State" mean Customer. Terms with initial letters capitalized that are not expressly defined in this Attachment have the meaning set forth in the AWS Enterprise Agreement.

### 2. State IT Policy and Standard Requirements

AWS and the State will comply with the standards outlined in the Agreement.

#### 2.1. State Information Technology Policies

As of the Effective Date, AWS is certified under ISO 27001 / ISO 27018 / ISO 27017 / ISO 9001] (the "Certification Standards"). AWS will maintain an information security program designed to provide at least the same level of protection as evidenced by its certification under each Certification Standard on the Effective Date.

"FedRAMP" means the Federal Risk and Authorization Management Program. "ATO" means authorization to operate. "FedRAMP Covered Services" means only the services listed as "in scope and is reflected in current reports" on the FedRAMP tab at <https://aws.amazon.com/compliance/services-in-scope/> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

As of the effective date, AWS offers FedRAMP Covered Services via AWS GovCloud (US) and AWS US East-West which have FedRAMP compliant systems that have been granted authorizations, have addressed the FedRAMP security controls (based on NIST SP 800-53 rev. 4), used the required FedRAMP templates for the security packages posted in the secure FedRAMP Repository, has been assessed by an accredited independent third party assessor (3PAO) and maintain continuous monitoring requirements of FedRAMP. FedRAMP Covered Services have varying degrees of ATO dependent on region and not all FedRAMP Covered Services available in one region are a necessarily available at another. The services in scope at a particular baseline as FedRAMP High or FedRAMP Moderate can be found at <https://aws.amazon.com/compliance/services-in-scope/>, as may be updated by AWS from time to time.

AWS offers a customizable and extendable capability based on open-standards APIs designed to enable integration with third party applications. The State understands and agrees that not all AWS Services meet the moderate or high level baseline described in this Section 2.1. Services are designed to provide the State's systems administrators with 24x7 visibility into the services through a web-based "dashboard" capability that enables them to monitor, in real or near real time, the Services' performance against published SLAs. Provided that Customer has support at the Enterprise or Business level, upon Customer request, AWS will use reasonable efforts to support and provide information to Customer on best practices for security policies and compliance.

AWS is responsible for maintaining the AWS Network and AWS Security Standards set forth in the Agreement. The manner in which AWS maintains and supports its infrastructure and security may be demonstrated by AWS through its SOC 1 Type II and SOC 2 Type II reports (collectively "SOC reports"). Provided that the parties have an applicable NDA in place, AWS will make this documentation available to Customer via AWS Artifact (or an alternative means accessible via the AWS Site) and this documentation will be treated as Confidential Information of AWS under the NDA.



2.1.1. State of Ohio Standards

The State may elect from Contractor various Service Offerings which are further described at <https://aws.amazon.com/> as may be updated by AWS from time to time. Upon request, Contractor will provide the State with access to whitepapers and information about how to design and architect its preferred solutions. Provided Customer is enrolled in AWS Support at the Enterprise-level tier or above, AWS will provide a designated Technical Account Manager who will provide advocacy, guidance to help plan and build solutions using best practices, and proactively assist to help keep your AWS environment operationally healthy. Additionally, in such case, the Technical Account Manager will use commercially reasonable efforts to meet regularly at mutually agreed times, which may be via telephone or teleconferencing to discuss the State’s use of the Services and this Agreement.

As of the Effective Date, AWS supports solutions designed to comply with the State’s supported Server / OS versions as identified in Table 1 below. The following are the State’s Required Server and OS versions:

**Table 1 – Supported Server /OS versions**

Operating System	Edition
Microsoft Windows Server	Standard and Datacenter
RedHat Linux	Enterprise
SUSE Linux	Enterprise
Oracle Enterprise Linux	Enterprise

3. State and Federal Data Privacy Requirements

Because the privacy of individuals’ personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public’s trust in working with the State, Contractor offers tools, services, or products designed to help the State manage its data in compliance with applicable laws and regulations. State Sensitive information is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of *personally identifiable information* that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, and Criminal Justice Information under Federal Bureau of Investigation’s Criminal Justice Information Services (CJIS) Security Policy. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

AWS offers services which Customer may use and configure in compliance with the Health Insurance Portability and Accountability Act (HIPAA) provided the Customer has a Business Associate Addendum in place between itself and AWS. The State is responsible for configuring and using the HIPAA Eligible Services consistent with HIPAA’s requirements. To the extent that personally identifiable information (PII) in a system is “protected health information” under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the Customer is responsible for implementing security protocols and practices consistent with the FIPPS principles in alignment with the HIPAA Privacy Rule. To the extent that there is PII in a system that is not “protected health information” under HIPAA, the FIPPS principles shall still be implemented by the Customer and, when applicable, aligned to other laws or regulations.



AWS offers HIPAA Eligible Services Which Customer may use when handling personally identifiable information in the system which qualifies as "protected health information" under the HIPAA Privacy Rule.

The Contractor offers Services which are designed to assist the State with complying with state and federal confidentiality and information disclosure laws, rules and regulations applicable to work associated with this Contract including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- Code of Federal Regulations for Public Health and Public Welfare: 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945, 45 CFR 164.502 (e) and 164.504 (e);
- Ohio Revised Code (ORC) 1347.01, 1347.04 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.99, 5160.39, 5168.13, and 5165.88; (and corresponding Ohio Administrative Code Rules and Updates as may be separately agreed upon by the parties in writing) To the extent applicable the State's operational control model, IT-SEC-02 Enterprise Security Control Framework, located at - <http://das.ohio.gov/Portals/0/DASDivisions/InformationTechnology/IG/pdf/ITS-SEC-02.pdf>, which is aligned to NIST SP 800-53 (current, published version).
- IRS Publication 1075, Tax Information Security Guidelines for federal, state and local agencies

### 3.1. Federal Tax Information

3.1.1. As of the Effective Date, AWS provides services, tools, and functionality that the State may use to architect a solution that is compliant with 26 C.F.R. §301.6103(n)-1(d); IRS Publication 1075 (Rev. 8-2010) (collectively the "IRS Rules") including the ability to meet Data Isolation, Data Privacy, Data Encryption, Risk Assessment, Data Destruction and Removal, and Security Control Implementation as defined in the IRS Rules. The Customer, using the AWS infrastructure as a service cloud offering to architect an IRS 1075-compliant solution, is responsible for using the cloud services in accordance with 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1; IRS Publication 1075 (Rev. 8-2010); and all applicable conditions and restrictions as may be prescribed by the IRS by regulation, published rules or procedures, or written communication to the State, or the State's agency or its contractor.

### 3.1.2. IRS 1075 Performance Requirements:

In performance of this contract, the State, the State's agency, or its contractor are responsible for complying with the following requirements:

- All work involving Federal Tax Information (FTI) will be done under the supervision of the State, the State's agency, or its contractor or their employees.
- To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI. The State acknowledges and understands that it is solely responsible for enabling security features and protecting against unauthorized use of and access to FTI.
- Any federal tax return or return information made available in any format shall be used only for the purposes of performing this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the State, the State's agency, or its contractor is prohibited.



- All federal tax returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- The State, the State's agency, or its contractor certify that the IRS data processed during the performance of this contract will be completely purged from all data storage components of its computer facility, and no output will be retained by the contractor after the work is completed. If immediate purging of all data storage components is not possible, the State, the State's agency, or the contractor certify that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosure.
- Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the State or its designee. When this is not possible, the State, the State's agency, or its contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the State or its designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
- The State, the State agency, or its contractor will maintain a list of employees authorized access. Such list will be provided to the State and, upon request, to the IRS reviewing office.
- The State or AWS, will have the right to void the contract if the State or the State agency, fails to provide the safeguards described above.

### 3.1.3. IRS 1075 Criminal/Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized 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. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material 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 the contract. Inspection by or disclosure to anyone without an official need-to-know 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. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.
3. 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 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.

For purposes of this section 3.1.2 of the Attachment, references to "Covered Services" means the commercially available services provided by AWS under this Agreement; and "Covered Entity" means any state or local government entity in the state of Ohio that purchases Covered Services from AWS under this Agreement. In the event the IRS desires to perform an assessment of the Covered Services to verify the State's compliance with the IRS Rules as they pertain to the State's use of the Covered Services, AWS will in good faith use commercially reasonable efforts to provide documentation and information as reasonably necessary to respond to such assessment. The IRS may be permitted to request that a Covered Entity provide access to data or content belonging to Covered Entities in connection with such assessment, but not data belonging to other customers in the multi-tenant environment from which the Covered Services are delivered. If the IRS identifies what it believes to be deficiencies in the Covered Services as a result of the assessment, AWS and the State are committed to working together in good faith to resolve the IRS's concerns through discussion and interaction between the State, AWS and the IRS. Should the participation of the Covered Entity be required, the State will coordinate such participation. Any information provided by AWS to the IRS or the State will be treated as Confidential Information and afforded the highest level of confidential treatment available under applicable law.

### 3.2 Remedies

The State has the remedies provided to it under the AWS Enterprise Agreement for Contractor's breach of the terms of this Attachment.

### 3.3 Prohibition on Off-Shore and Unapproved Access

AWS provides Services designed to enable Customer to maintain and secure their data within the United States. AWS understands and will abide by the requirements of Ohio Executive Order 2011-12K provided Customer will at all times only select a US region for the Customer Content and will not ever select an AWS Region outside of the continental US. Customer warrants that at all times it will only select US based regions for the AWS Services. AWS provides FedRAMP Covered Services available as further described in Section 2.1 of this Attachment. FedRAMP Covered Services means only the services listed as "in scope and is reflected in current reports" on the FedRAMP tab at <https://aws.amazon.com/compliance/services-in-scope/> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time. The Parties understand that AWS may add regions that may or may not be FedRAMP certified.

AWS offers Services designed to enable the State to comply with applicable U.S. statutes, regulations, and administrative requirements regarding its relationships with non-U.S. governmental and quasi-governmental entities including, but not limited to the export control regulations of the International Traffic in Arms Regulations ("ITAR") and the Export Administration Act ("EAA"); the anti-boycott and embargo regulations and guidelines issued under the EAA, and the regulations of the U.S. Department of the Treasury, Office of Foreign Assets Control, HIPAA Privacy Rules and other conventions as described and required in this Supplement. As of the Effective Date, AWS offers use of some of its Services via the AWS GovCloud region. The AWS GovCloud region supports compliance with ITAR and provides an environment that is physically located in the US, and access by AWS personnel is limited to US Citizens.

Subject to the Section 3.3 of the AWS Enterprise Agreement, AWS will not move Customer Content from the regions selected by Customer, if Customer selects a US region then AWS will not move Customer Content from that region; 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).

### 3.4 Background Checks

AWS represents to the State that, as part of pre-employment screening practices for U.S. candidates with conditional offers of employment, AWS (directly or through its affiliates) maintains a policy of conducting criminal background checks (as permitted by applicable law) commensurate with the employment candidate's offered position ("Pre-Employment Background Check"). AWS will not permit a U.S. employment candidate to provide AWS Professional Services if such individual's Pre-Employment Background Check results fail to meet AWS's (or its affiliates') standards for employment. The following searches are currently conducted for U.S. candidates that will be performing AWS Professional Services on-site at a Customer's location:

- a federal crimes search for all federal districts in which the candidate has lived in the past 7 years as determined by a self-report and his/her Social Security Number (SSN) search);
- a felony and misdemeanor search of all county courts in counties in which the candidate has lived in the past 7 years as determined by a self-report and the SSN search), provided that for former addresses located within AL, AK, AR, CO, CT, DC, DE, ID, MD, MN, NE, NJ, NM, NY, NC, ND, OR, RI, SD, UT, WA, or WI only, a "statewide" search is permitted in lieu of a county court search; and
- searches of the Sex Offender Registry and Office of Foreign Assets Control (OFAC).
- Any and all additional requirements relating to background checks for AWS employees handling Criminal Justice Information (CJI) will be set forth in a separate agreement governing CJI to be entered into between AWS and the State or the State's designated State agency.

#### 4. State Security and Information Privacy Standards and Requirements

AWS will be responsible for maintaining information security in accordance with obligations expressly set forth on AWS in the Agreement. The State may elect to receive security notifications through a central point of contact designated by the State in the AWS Management Console.

The Contractor's responsibilities with respect to Security Services will include the following:

- Develop, maintain, update, and implement security procedures, including physical access strategies and standards, ID approval procedures and a breach of security action plan which AWS may demonstrate through SOC 1 Type II and SOC 2 Type II reports and the FedRAMP SSP. Upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will provide to Customer a copy of its System and Organization Controls 1 (SOC 1) Type 2 Report or such alternative industry standard reports or certifications that are substantially equivalent as reasonably determined by AWS. AWS will provide this documentation no more than twice annually and this documentation will be treated as Confidential Information of AWS under the NDA.
- So long as Customer is enrolled in Enterprise Support, AWS will (at Customer's request) assist Customer with researching system security problems.
- Perform physical security functions (e.g., identification badge controls, alarm responses) at the facilities under the Contractor's control.
- Provide effective patch management designed to ensure patching is up to date and flaws are fixed with the infrastructure.
- Provide effective configuration management of infrastructure devices appropriately configured in accordance with policy.
- Will perform an annual relevant role based security training for relevant security personnel

The State will:

- Develop, maintain and update the State IT Security Policies, including applicable State information risk policies, standards and procedures.
- Provide the contractor with contact information for security and program personnel for incident reporting purposes.
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies provided such complies with AWS standards including providing AWS notice prior to State performing such scanning.
- Provide the State security audit findings material for the Services based upon the security policies, standards and practices in effect as of the Effective Date and any subsequent updates.

#### 4.1 Protection of State Data

**Protection of State Data.** Customer Content may contain "State Data" which includes all data and information the State transfers to AWS for processing, storage, or hosting by the Services in connection with an AWS Enterprise Account, including, but not limited to sensitive Customer information which may include PII or SII if Customer elects. To the extent State Data qualifies as Customer Content, AWS will treat State Data in accordance with Section 3 of the AWS Enterprise Agreement. 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 of the AWS Enterprise Agreement, 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 Section 3 of the AWS Enterprise Agreement, to enable Customer to seek a protective order or other appropriate remedy.

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

#### Handling the State's Data

To the extent State Data qualifies as Customer Content, AWS will handle such data in accordance with the rights and restrictions set forth in Section 3 of the AWS Enterprise Agreement as referenced in the above Section 4.1 of this Attachment.

#### 4.2 Contractor Access to State Networks Systems and Data

The Contractor provides a robust set of boundary security tools that incorporate generally recognized best practices.

To implement these, the Customer must:

- Use the Services and architect its solution in accordance with AWS security best practices set forth at [https://d1.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Best\\_Practices.pdf](https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf).
- Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable information.
- Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data.



On its part, AWS will not transfer Customer Content to a portable computing device except as requested or designated by Customer in writing which may be via the AWS Management Console. All handling of Customer Content by AWS will be in accordance with Section 3 of the AWS Enterprise Agreement. AWS will have a business continuity plan in place that address procedures for responding to issues with the AWS Network within AWS' control. Additionally, as of the Effective Date, AWS' SOC 1 Report includes (a) a description of the controls AWS operates for its business continuity plan, (b) confirmation that AWS tests and updates its business continuity plan at least annually, and (c) a description of any deficiencies identified in AWS's business continuity plan, together with details of the proposed steps taken or to be taken to remediate such deficiencies. AWS' business continuity and disaster recovery program encompasses processes and procedures for identification, response, and recovery from a Force Majeure Event; any other event that causes a material disruption to the provision of a material portion of the Services, or major event or incident within the AWS environment. This program incorporates availability, redundancy, and infrastructure capacity planning within its standards, and is integrated into AWS' risk management program. Customers can refer to the AWS SOC 2 Report.

#### **Limited Use; Survival of Obligations.**

AWS may use Customer Content only as authorized by the Agreement and for no other purpose. During the 90 days following the Termination Date of this Agreement, 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.

#### **4.3 Periodic Security and Privacy Audits**

The State may conduct its own periodic internal audit of the State's internal systems and the security, privacy, and access controls it chooses to deploy ("Internal Audit") in connection with its use of the AWS Services however the State does not have the right to conduct any on-site audits of AWS, audits of the AWS Network or of the AWS Services. Third party audit reports are available via SOC 1 Type II and SOC 2 Type II reports which AWS will provide to Customer in accordance with Section 2.1 of this Attachment. The State may conduct its Internal Audit provided it conforms with the requirements set forth in this Attachment, does not implicate or require access to data or accounts belonging to any other customers including other customers in the multi-tenant environment from which the Services are delivered, and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit or the Auditor of the State, depending on the focus area of an audit. Should an audit issue or finding be discovered, the following resolution path shall apply:

- If a security or privacy issue exists in any of the IT resources furnished to AWS by the State (e.g., code, systems, computer hardware and software), the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue, the State may elect to contract with AWS under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of AWS. AWS is responsible for resolving security or privacy issues with respect to the Security Standards set forth in Attachment A of the Agreement provided resolving such issue is within AWS's control and commercially reasonable and such issues are identified by an AWS selected third party assessment organization; provided nothing in this section modifies Customer's obligations under Section 4.1 of the AWS Enterprise Agreement.

#### **4.4 State Penetration and Controls Testing**

The state may, at its sole discretion, elect to perform penetration testing provided such penetration testing is conducted in accordance with AWS's Penetration Testing Policy (available at <http://aws.amazon.com/security/penetration-testing/> or any successor or related locations designated by AWS). Requests will be made in the manner described by the Penetration Testing Policy, or in such other manner as AWS reasonably directs.

#### **4.5 Annual Security Plan: State and Contractor Obligations**



Upon request and provided the parties have an applicable NDA in place, AWS will provide the Customer a copy of the FedRAMP partner SSP for applicable regions up to two times in a calendar year. The Customer will develop, implement and thereafter maintain annually a Security Plan, that is in alignment with the National Institute of Standards and Technology ("NIST") Special Publication (SP) 800-53 (current, published version), for review, comment and approval by the State Information Security and Privacy Officers.

As of the Effective Date, AWS is certified under ISO 27001 / ISO 27018 / ISO 27017 / ISO 9001] (the "**Certification Standards**"). AWS will maintain an information security program designed to provide at least the same level of protection as evidenced by its certification under each Certification Standard on the Effective Date.

AWS as of the effective date, AWS provides Services that meet FedRAMP compliance standards as described in Section 3.3 of this Attachment. The State may refer to <https://aws.amazon.com/compliance/services-in-scope/> for a list of AWS Services that meet the scope of FedRAMP Moderate and FedRAMP High.

#### 4.6 Open API's

Contractor provides Services accessible via APIs. Proposed vendor applications must describe in detail all available features and functionality accessible via APIs.

#### 4.7 Boundary Defenses

The Contractor provides tools designed to assist the Customer with:

- supporting the denial of communications to/from known malicious IP addresses\*
- Ensuring that the System network architecture separates internal systems from DMZ and extranet systems
- Requiring remote login access to use two-factor authentication
- Supporting the State's monitoring and management of devices remotely logging into internal network
- Supporting the State in the configuration firewall session tracking mechanisms for addresses that access system

#### 4.8 Audit Log Reviews

So long as the Customer has purchased Enterprise Support or higher level of support services then the Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Assist Customer with information and guidance on how to configure systems and environments to have adequate space to store logs
- Work with the State to devise and implement profiles of common events from given systems to both reduce false positives and rapidly identify active access
- Assist the State on understanding how to configure operating systems to log access control events
- Provide guidance to the State on how to design and execute bi-weekly reports to identify anomalies in system logs
- Provide guidance on how to leverage WORM technology

#### 4.9 Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues

**General Security Breach Notification.** If AWS knows of a breach of the security measures described in the AWS 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 (x) notify

Customer of the Security Event using the email address listed in Customer's AWS account within 48 hours after AWS confirms the Security Event (provided Customer's AWS Account is enrolled in Business or Enterprise-level AWS Support plan and AWS is not prohibited from providing the notification by a court order or other legal requirement) and (y) promptly take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Event. If requested by Customer, AWS will provide Customer with reasonable and appropriate details relevant to the cause, nature and Customer impact of the Security Event; provided, that AWS will not be required to provide this information if (a) Customer is not enrolled in AWS Support at the Business or Enterprise level or (b) AWS reasonably determines the disclosure would prejudice AWS's security or violate applicable law.

**Response to Suspected Security Events.** AWS will maintain an information security program that requires AWS security personnel that observe conditions which lead them to reasonably suspect a Security Event has occurred or is occurring (such conditions being a "Suspected Security Event") to take at least the following actions: (a) Suspected Security Events will be internally reported by AWS security personnel as quickly as reasonably practicable, (b) Suspected Security Events will be reported through appropriate management channels in a manner that is appropriate and consistent with AWS reporting policies; and (c) Suspected Security Events will be assessed in a reasonably prompt manner to determine whether they are to be classified as Security Event.

**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 and Customer will 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 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) **Confidentiality and Costs.** Customer will undertake to obtain confidential treatment or similar protection for any information disclosed to, or gathered by, Regulator under this Section. Customer will reimburse AWS and its Affiliates for their costs and expenses related to a Request.

For purposes of this section "Regulator" means the State Inspector General, State Office of Information Technology Chief Information Security Officer, Office of Budget & Management Office of Internal Audit, Auditor of the State of Ohio, or a government or regulatory body with binding authority to regulate Customer's financial or healthcare service 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).

#### 4.10 Requirements Overview

Offerors responding to State issued RFQ/RFP requests, and as Contractors performing the work following an award, are required to propose solutions that comply with the standards outlined in this document. In the event Offeror finds it necessary to deviate from any of the standards, a variance may be requested, and the Offeror must show sufficient business justification for the variance request. The Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.



**Exhibit 1- State Entities**

**Amazon Web Services MCSA0080**

**Exhibit 1**

Cabinet Level Superintended State Agencies
AJUTANT GENERAL
ADMINISTRATIVE SERVICES
BOARD OF REGENTS
BUR OF WORKERS' COMPENSATION
DEPARTMENT OF VETERANS' SERVIC
DEPT OF AGING
DEPT OF AGRICULTURE
DEPT OF COMMERCE
DEPT OF HEALTH
DEPT OF NATURAL RESOURCES
DEPT OF PUBLIC SAFETY
DEPT OF REHAB & CORRECTIONS
DEPT OF TAXATION
DEPT OF TRANSPORTATION
DEPT OF YOUTH SERVICES
DEVELOPMENTAL DISABILITIES
OHIO DEVELOPMENT SERVICES AGENCY
ENVIRONMENTAL PROTECTION AGCY
INSURANCE
JOB AND FAMILY SERVICES
LOTTERY COMMISSION
MEDICAID
MENTAL HEALTH AND ADDICTION SERVICES
OFFICE OF BUDGET & MGMT



Other Superintended State Agencies
ACCOUNTANCY BOARD OF OHIO
AIR QUALITY DEVELOPMENT AUTH
ATHLETIC COMMISSION
BD OF EXAMINERS OF ARCHITECTS
BOARD OF BARBER EXAMINERS
BOARD OF COSMETOLOGY
BOARD OF DIETETICS
BOARD OF ENGINEERS & SURVEYORS
BOARD OF NURSING
BOARD OF OPTOMETRY
BOARD OF PHARMACY
BOARD OF PSYCHOLOGY
BOARD OF TAX APPEALS
BROADCAST EDUCATIONAL MEDIA COMMISSION
CAREER COLLEGES/SCHOOLS BOARD
CASINO CONTROL COMMISSION
CHEMICAL DEPENDENCY PROFS
CHIROPRACTIC EXAMINERS BOARD
CIVIL RIGHTS COMMISSION
COMMISSION ON MINORITY HEALTH
COMMISSION ON SERVICE & VOLUNT
COUNSELOR & SOCIAL WORKERS BD
DENTAL BOARD
DEPARTMENT OF VETERANS' SERVIC
ELECTIONS COMMISSION
EMBALMERS & FUNERAL DIR BOARD
EMPLOYMENT RELATIONS BOARD
ENVIRONMENTAL BOARD OF REVIEW
ETHICS COMMISSION
HISPANIC-LATINO AFFAIRS COMM
INDUSTRIAL COMMISSION
JOINT COMM ON AGCY RULE REVIEW
LAKE ERIE COMMISSION
LIBRARY BOARD



Other Superintended State Agencies
LIQUOR CONTROL COMMISSION
MANUFACTURED HOMES COMMISSION
MEDICAL BOARD
MOTOR VEHICLE COLLISION REPAIR
OCC/PHYS THERAPY/ATHLETIC TRNR
OFC OF INSPECTOR GENERAL
OFFICE OF CONSUMERS' COUNSEL
OHIO ARTS COUNCIL
OHIO EXPOSITIONS COMMISSION
OHIO FACILITIES CONSTRUCTION COMMISSION
OHIO SCHOOL FOR THE BLIND
OHIO SCHOOL FOR THE DEAF
OPPORTUNITIES FOR OHIOANS WITH DISABILITIES
OPTICAL DISPENSERS BOARD
ORTHOTIC PROSTHETIC PEDORTHICS
PUBLIC DEFENDER COMMISSION
PUBLIC WORKS COMMISSION
RACING COMMISSION
RESPIRATORY CARE BOARD
SANITARIAN REGISTRATION BOARD
SO OHIO AGR/COMM DEVELOPMENT
SPEECH-LANGUAGE PATH/AUD BOARD
VETERINARY MEDICAL BOARD

Non Superintended Legislative, Judicial, and Elected Entities
ATTORNEY GENERAL
AUDITOR OF STATE
CAPITAL SQUARE REVIEW & ADV BD
COURT OF CLAIMS
HOUSE OF REPRESENTATIVES
JOINT LEGIS ETHICS COMMITTEE



JUDICIAL CONFERENCE OF OHIO
JUDICIARY / SUPREME COURT
LEGISLATIVE SERVICE COMMISSION
OFFICE OF THE GOVERNOR
SECRETARY OF STATE
SENATE
TREASURER OF STATE



**Exhibit 2 – Sample Report for Cooperative Purchasing Member Services**

Example Quarterly Report for Cooperative Purchasing Members:

Vendor Name:	Amazon Web Services, Inc.								
Contract Number:	MCSA0080								
Submitted Reporting Quarter:	State Fiscal Year 2018 - Q2								
Customer Name (Customer's Proper Name)	Cooperative Purchasing Member or State Entity	PO Number	Sales Period (i.e., State Fiscal quarter usage)	Description	Quarterly Customer Sales (pre-credits)	Customer's Billing Address	City	State	Zip Code
<b>Total Quarterly Sales:</b>					0.00				
<b>Total all Admin fees due:</b>					0.00				

Example for illustrative purposes only:

Vendor Name:	Amazon Web Services, Inc.								
Contract Number:	MCSA0080								
Submitted Reporting Quarter:	State Fiscal Year 2018 - Q2								
Customer Name (Customer's Proper Name)	Cooperative Purchasing Member or State Entity	PO Number	Sales Period (i.e., State Fiscal quarter usage)	Description	Quarterly Customer Sales (pre-credits)	Customer's Billing Address	City	State	Zip Code
Oho Department of IT	State Entity	1111	Q2 2018	Cloud Hosting Services	100.00	496 Broad Street	Columbus	OH	43215
City of XYZ, Dept. of Finance	Cooperative Purchasing Member	2222	Q2 2018	Cloud Hosting Services	75.00	123 Broad Street	Columbus	OH	43215
City of ABC, Department of Finance	Cooperative Purchasing Member	2222	Q2 2018	Cloud Hosting Services Support	25.00	789 Broad Street	Columbus	OH	43215
ABC Public Schools	Cooperative Purchasing Member	3333	Q2 2018	Cloud Hosting Services	1,200.00	123 Reading Lane	Cincinnati	OH	45201
<b>Total Quarterly Sales:</b>					1,400.00				
<b>Total all Admin fees due:</b>					0.00				

