AGREEMENT FOR SERVICES

This Agreement for Services (hereinafter "Agreement") is made and entered by and between the State of Ohio, acting by and through the Ohio Department of Agriculture (hereinafter "ODA"), located at 8995 East Main Street, Reynoldsburg, Ohio 43068, and Acclaim Systems, Inc. (hereinafter "Contractor"), located at 110 East Pennsylvania Blvd., Feasterville, Pennsylvania 19053. In consideration of the mutual promises and obligations contained herein, the parties agree by and between themselves as follows:

Article I – Statement of Work

1. Contractor agrees to undertake and complete the work and activities set forth in the Statement of Work – State Vet: AgEnterprise State Vet Module, attached hereto as ***Exhibit A*,** made a part hereof, and incorporated herein by reference as if fully rewritten herein.

2. Specifically, Contractor agrees to provide software maintenance, support and problem resolution of AgEnterprise for ODA Animal Health from July 1, 2025 to June 30, 2026 (FY 2026) and July 1, 2026 to June 30, 2027 (FY 2027) as described in ***Exhibit A***.

3. ODA may, from time to time as it deems appropriate and necessary, communicate specific instructions and requests to Contractor concerning the performance of the work described herein. Upon such notice and within a reasonable time, Contractor shall make reasonable attempts to comply with such instructions and fulfill such requests to the satisfaction of ODA. It is expressly understood by ODA and Contractor that the instructions and requests are for the sole purpose of performing the specific tasks requested and to ensure satisfactory completion of the work described herein. However, the instructions and requests are not intended to amend or alter the terms of this Agreement or any part thereof.

Article II - Term and Location of Performance

1. Term. This Agreement shall be effective on **July 1, 2025,** or the date all provisions of Section 126.07 of the Ohio Revised Code are met, whichever is later, and shall expire on **June 30, 2027**. This Agreement shall remain in effect until the ending date stated in the Agreement unless earlier terminated pursuant to the terms of the Agreement.

2. Location of Performance; Prohibition of Expenditure of Public Funds for Offshore Services. No State Cabinet Agency, Board or Commission will enter into any agreement to purchase services provided outside of the United States or that allows State Data to be sent, taken, accessed, tested, maintained, backed-up, stored, or made available remotely outside (located) of the United States, unless a duly signed waiver from the State has been attained. Notwithstanding any other terms of this Agreement, the State reserves the right to recover any funds paid for services the Contractor performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights and remedies provided to the State in the Agreement.

   Further, no State agency, board, commission, State educational institution, or pension fund will make any purchase from or investment in any Russian institution or company. Notwithstanding any other terms of this Agreement, the State reserves the right to recover any funds paid to Contractor for purchases or investments in a Russian institution or company in violation of this paragraph. The provisions of this paragraph will expire when the applicable Executive Order is no longer effective.

   The Contractor must complete the Contractor/Subcontractor Affirmation and Disclosure Form affirming the Contractor understands and will meet the requirements of the above prohibition. During

the performance of this Agreement, if the Contractor changes the location(s) disclosed on the Affirmation and Disclosure Form, Contractor must complete and submit a revised Affirmation and Disclosure Form reflecting such changes.

Article III - Compensation

1. In consideration of the promises of Contractor herein, and as compensation for the obligations undertaken by Contractor, ODA shall pay Contractor Seventy-One Thousand One Hundred Seventy-Four Dollars and 34/100 Cents ($71,174.34) for the work described in ***Exhibit A***.

    a. **The total compensation under this Agreement shall not exceed Thirty-Four Thousand Five Hundred Ninety-Nine Dollars and 34/100 Cents ($34,599.34) in FY26.**

    b. **The total compensation under this Agreement shall not exceed Thirty-Six Thousand Five Hundred Seventy-Five Dollars and 00/100 Cents ($36,575.00) in FY27.**

2. Taxes. Pursuant to Section 5739.02 of the Ohio Revised Code, the State is exempt from sales tax. Pursuant to Section 5741.02(C) of the Ohio Revised Code, the State is exempt from use tax.

3. Travel. Any travel that Contractor requires to perform its obligations under this Agreement will be at the Contractor's expense.

4. Payment Due Date. Unless otherwise stated in this Agreement, and in accordance with Section 126.30 of the Ohio Revised Code, payments under this Agreement will be due on the 30th calendar day after the date of actual receipt of a proper invoice by the ODA. The date payment is issued by ODA will be considered the date payment is made.

5. Invoice Requirements. The Contractor authorized to submit invoices must submit an invoice to the ODA. The Contractor will only be compensated for the deliverables received and accepted by the ODA. To be a proper invoice, the invoice must include the following: Contractor's name and address, invoice date, the date services were provided, itemization of supplies or services provided, including costs, and clear statement of total payment expected.

    The adequacy and sufficiency of all invoices shall be determined solely by the ODA. If ODA determines that an invoice is inadequate or insufficient or determines that further documentation or clarification is required for a particular invoice, the burden of providing the required information or documentation is on the Contractor. Costs incurred by the Contractor that are associated with providing the required additional information or documentation and costs, in relation to defending an inadequate or insufficient invoice shall not be charged to the ODA and shall not be considered an allowable expense under this Agreement.

6. Appropriation of Funds. ODA's funds are contingent upon the availability of lawful appropriations. If the General Assembly or any third-party providing funding fails at any time to continue funding the payments or any other financial obligations due by ODA under this Agreement, ODA will be released from its obligations on the date funding expires. If appropriations are approved, ODA may continue this Agreement past the current biennium by issuing written notice of continuation to the Contractor. Any obligations of ODA are subject to Section 126.07 of the Ohio Revised Code.

7. Certification of Funds. None of the duties or obligations in this Agreement are binding on ODA, and the Contractor will not begin performance on this Agreement, until all of the following conditions are met:

    a. All statutory provisions under the Ohio Revised Code have been met.

b. All necessary funds are made available by the ODA.

c. If applicable, an official State of Ohio Purchase Order ("P.O.") has been issued from the ODA.

d. If required, the Controlling Board of Ohio has approved the purchase in accordance with Section 127.16 of the Ohio Revised Code.

Article IV - Data Security and Privacy Terms

Contractor shall comply with the data security and privacy terms attached hereto as ***Exhibit B***, which are incorporated into this Agreement by reference as if fully rewritten herein to the extent they apply to the products and services provided under this Agreement.

Article V – Termination of Agreement

1. Termination for Convenience. ODA may terminate this Agreement, in whole or in part, at any time and for any reason by giving a fourteen (14) calendar day written notice to Contractor. Upon notice of termination, Contractor shall cease all work under this Agreement and shall take all necessary or appropriate steps to limit disbursements and minimize costs in ceasing all work. Contractor shall be required to furnish a report setting forth the status of all activities under this Agreement including but not limited to the work completed and such other information as ODA may require.

2. Termination for Breach. ODA shall be entitled, by written or oral notice, to cancel this Agreement in its entirety or in part immediately, for breach of any of the terms, and to have all other rights against Contractor by reason of Contractor's breach as provided by law.

    a. A breach shall mean, but shall not be restricted to, any one or more of the following events:

        i. Contractor breaches any warranty, or fails to perform or comply with any term of this Agreement;

        ii. In ODA's sole opinion, Contractor becomes insolvent or in an unsound financial condition so as to endanger performance hereunder; or

        iii. Contractor becomes the subject of any proceeding under any law relating to bankruptcy, insolvency, reorganization or relief from debtors.

    b. No term or provision of this Agreement shall be deemed waived and no breach excused unless the waiver of consent is in writing by both parties to this Agreement. ODA may at its discretion, in event of breach, notify the Contractor of the breach and allow it a time specified by ODA to correct the breach.

3. Force Majeure

    a. The term "force majeure" as used herein shall mean without limitation: acts of God, such as epidemics; earthquakes; fire; storms; hurricanes; tornadoes; floods; washouts; droughts; or other severe weather disturbances; explosions; arrests; restraint of government and people; war; strikes; and other such events or any causes which could not be reasonably foreseen in the exercise of ordinary care, and which is beyond the reasonable control of the party affected and said party is unable to prevent.

    b. If by reason of force majeure the Contractor is unable, in whole or in part, to perform under

this Agreement, the Contractor shall not be in breach of contract during the continuance of such inability. The Contractor shall, however, remedy, with all reasonable dispatch such cause preventing the Contractor from carrying out the obligations under this Agreement. Except as otherwise provided herein, neither the Contractor nor ODA shall be liable to the other for any delay or failure of performance of any provisions contained herein, nor shall any such delay or failure of performance constitute default hereunder, to the extent that such delay or failure is caused by force majeure.

Article VI - Indemnification

1. General Indemnity. The Contractor must indemnify ODA for all liability and expense arising out of the performance of this Agreement, provided that such liability or expense is due to the negligence or other tortious conduct of the Contractor, its employees, agents, or subcontractors. The Contractor will not be responsible for any damages of liability to the extent caused by the negligence or willful misconduct of ODA, its employees, other contractors or agents.

2. Contractor shall notify ODA immediately upon commencement of any legal actions brought against Contractor whose outcome may affect the rights of the ODA granted under this Agreement. ODA shall have the right at its own expense to appear in and defend such actions.

3. In the event legal action is instituted by ODA for any default on the part of Contractor, and Contractor is adjudged by a court of competent jurisdiction to be in default, Contractor shall pay to ODA all costs and expenses expended or incurred by ODA and reasonable attorney's fees.

Article VII - Records Maintenance and Access

1. Maintenance of Records. Contractor shall establish and maintain for at least three (3) years after the last day of the Term of this Agreement or earlier termination of this Agreement its records regarding this Agreement, including, but not limited to, financial reports, and all other information pertaining to Contractor's performance of its obligations under this Agreement. Contractor also agrees that any records required by ODA with respect to any questioned costs, audit disallowances, litigation or dispute between ODA and Contractor shall be maintained for the time needed for the resolution of such question or dispute.

2. Inspection and Copying. At any time during normal business hours and upon not less than twenty-four (24) hours prior written notice, Contractor shall make available to ODA, its agents or other appropriate State agencies or officials all books and records regarding this Agreement which are in the possession or control of Contractor, including, but not limited to, financial reports, and all other information pertaining to Contractor's performance of its obligations under this Agreement. ODA, its agents and other appropriate State agencies and officials may review, audit and make copies of such books and records. Any such inspection of books and records will be undertaken in such a manner as not to interfere unreasonably with the normal business operations of Contractor.

Article VIII - Independent Contractor

1. It is fully understood and agreed that Contractor is an independent contractor and is not an agent, servant, or employee of ODA, and that neither has the authority to bind the other to any third person or otherwise to act in any way as the representative of the other.

2. Contractor declares that it is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including, but not limited to, any insurance coverage, workers' compensation, or unemployment compensation that is

required in the normal course of business and will assume all responsibility for any federal, state, municipal or other tax liabilities. Additionally, Contractor understands that as an independent contractor, it is not a public employee and is not entitled to contributions from the State to any public employee retirement system.

Article IX - Adherence to State and Federal Laws, Regulations

1. Compliance with Law. Contractor must comply throughout the duration of the Agreement with all applicable federal, state, and local laws and Executive Orders while performing under this Agreement.

2. Governing Law. This Agreement shall be governed by the laws of the State of Ohio, and the venue for any disputes will be exclusively with the appropriate court in Franklin County, Ohio.

3. Conflict of Interest/Ethics Laws. Contractor represents, warrants and certifies that it and its employees engaged in the administration or performance of this Agreement are knowledgeable of and understand the Ohio Ethics and Conflict of Interest laws including but not limited to Chapter 102 and Sections 2921.42 and 2921.43 of the Ohio Revised Code. Contractor further represents, warrants, and certifies that neither Contractor nor any of its employees will do any act that is inconsistent with such laws or otherwise presents a conflict of interest.

4. Campaign Contributions. Unless this Agreement was solicited by competitive bid pursuant to Section 125.07 of the Ohio Revised Code, Contractor hereby certifies that all applicable parties are in full compliance with Section 3517.13 of the Ohio Revised Code.

5. Drug-Free Workplace Compliance. The Contractor agrees to comply with all applicable state and federal laws regarding drug-free workplace and shall make a good faith effort to ensure that all Contractor employees, while working on State property or performing work on behalf of the State, will not purchase, transfer, use, be under the influence of, or possess illegal drugs, non-medical cannabis (recreational marijuana), or alcohol, or abuse prescription drugs or medical marijuana in any way.

6. Trade. Pursuant to Section 9.76(B) of the Ohio Revised Code, Contractor warrants that Contractor is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the Agreement period.

   The State of Ohio does not acquire supplies or services that cannot be imported lawfully into the United States or transact business with any entity or individual subject to financial sanctions imposed by the United States. The Contractor certifies that it, its subcontractors, and any agent of the Contractor or its subcontractors, will acquire any supplies or services in accordance with all trade control laws, regulations or orders of the United States, including the prohibited source regulations set forth in subpart 25.7, Prohibited Sources, of the Federal Acquisition Regulation and any sanctions administered or enforced by the U.S. Department of Treasury's Office of Foreign Assets Control. A list of those entities and individuals subject to sanctions can be found at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists. These sanctions generally preclude most transactions involving Cuba, Iran, and Sudan, and most imports from Burma or North Korea.

7. Debarment. Throughout the Agreement term, the Contractor represents and warrants that neither it, nor any of its subcontractors, are debarred from consideration for contract awards by any governmental agency. If this representation and warranty is found to be false on the date the parties

signed this Agreement, this Agreement is *void ab initio*, and the Contractor must immediately repay any funds paid under this Agreement.

Article X - Warranties

1. Contractor warrants that it has the necessary background, training and skills to provide ODA with the essential services required and will provide its best efforts in the performance of its services set forth in ***Exhibit A*** and this Agreement. Best efforts shall be defined as being efforts performed in a workmanlike manner according to the highest professional standard for the purpose intended.

2. Unresolved Findings. Contractor warrants that it is not subject to an unresolved finding for recovery under Section 9.24 of the Ohio Revised Code. If the warranty is false on the date the parties signed this Agreement, the Agreement is void *ab initio*, and the Contractor shall immediately repay any funds paid under this Agreement.

3. Outstanding Judgments. Contractor warrants that it has no outstanding final judgments against it by the State of Ohio, including tax liabilities, and agrees that any payments incurred by the State in this Agreement may be applied against such liabilities currently owing or incurred in the future.

4. Unfair Labor Practice. Contractor warrants that it is not listed with the Ohio Secretary of State for unfair labor practices, pursuant to Section 121.23 of the Ohio Revised Code.

5. Acknowledgment. Contractor agrees that if any of the representations and warranties set forth within this Article is deemed to be false, this Agreement shall be void *ab initio*, and funds paid by ODA hereunder shall be immediately repaid to ODA.

Article XI - Miscellaneous

1. Entire Agreement. This Agreement and its exhibits and any documents referred to herein constitute the complete understanding of the parties and merge and supersede any and all other discussions, agreements and understandings, either oral or written, between the parties with respect to the subject matter hereof.

2. Severability. Whenever possible, each provision of this Agreement shall be interpreted in such a manner as to be effective and valid under applicable law, but if any provision of this Agreement is held to be prohibited by or invalid under applicable law, such provision shall be ineffective only to the extent of such prohibition or invalidity, without invalidating the remainder of such provisions of this Agreement.

3. Notices. All notices, invoices, consents, demands, requests and other communications which may or are required to be given hereunder shall be in writing and shall be deemed duly given if personally delivered or sent by United States mail, registered or certified, return receipt requested, postage prepaid, to the addresses set forth hereunder or to such other address as the other party hereto may designate in written notice transmitted in accordance with this provision.

   In case of ODA, to:

   Ohio Department of Agriculture
   Attn: Jon Cook
   8995 East Main Street
   Reynoldsburg, Ohio 43068

In case of Contractor, to:

Acclaim Systems, Inc.
Attn: Rakesh Khetawat
110 E. Pennsylvania Blvd
Feasterville, Pennsylvania 19053
Rakeshk@acclaimsystems.com

Notwithstanding the foregoing, ordinary communications regarding the status of services being provided by Contractor may be sent by electronic mail to the designated representatives of ODA and Contractor.

4. Amendments or Modifications. Either party may at any time during the term of this Agreement request amendments or modifications. Requests for an amendment or modification of this Agreement shall be in writing and shall specify the requested changes and the justification for such changes. Should the parties consent to modify the Agreement, then an amendment shall be drawn, approved, and executed in the same manner as the original agreement. The amendment must be signed by both parties to be effective.

5. Headings. The headings contained in this Agreement are inserted for convenience only and will not affect the interpretation of any of the Agreement terms and shall not be deemed to be a part of this Agreement.

6. Assignment. Neither this Agreement nor any rights, duties, or obligations described herein shall be assigned or subcontracted by Contractor without the prior express written consent of ODA.

7. Electronic Signatures. Copies of signatures sent by facsimile transmission or provided electronically in portable document format ("PDF") shall be deemed to be originals for purposes of execution and proof of this Agreement.

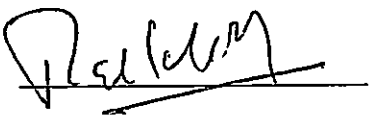
8. Public Records and Retention of Documents and Information. The Contractor acknowledges, in accordance with Section 149.43 of the Ohio Revised Code, that this Agreement, as well as any information, deliverables, records, reports, and financial records related to this Agreement are presumptively deemed public records. The Contractor understands that these records will be made freely available to the public unless ODA determines that, pursuant to state or federal law, such materials are confidential or otherwise exempt from disclosure. The Contractor must comply with any direction from the ODA to preserve and/or provide documents and information, in both electronic and paper form, and to suspend any scheduled destruction of such documents and information. Should the Contractor receive a public records request or subpoena with respect to any State Data, including personally identifiable information or confidential data, the Contractor will immediately notify ODA and fully cooperate with ODA's directions regarding such request.

9. Order of Priority: In the event of any conflict, contradiction, or ambiguity between the terms and conditions of this Agreement and any attachments to this Agreement, then the terms and conditions of this Agreement shall prevail over attachments or other writings.

10. Ohio Revised Code §9.27. Any provision, term, or condition in ***Exhibit A*** that violates or is contrary to Ohio law, including but not limited to, §9.27 of the Ohio Revised Code, is automatically void *ab initio* and thus unenforceable.

IN WITNESS WHEREOF, the parties have executed this Agreement on the last day and year set forth below.

CONTRACTOR,
Acclaim Systems, Inc.

By:  Date: 5/1/25

STATE OF OHIO,
Ohio Department of Agriculture ("ODA")

By: _____ Date: _____
Brian Baldridge
Director, ODA

EXHIBIT A

ABSTRACT

State Vet: AgEnterprise State Vet Module

John Kucek
Acclaim Systems

Executive Summary

In this statement of work, we detail the scope, tasks, and pricing for continuing Software Maintenance, Support and Problem Resolution, of **AgEnterprise** for Ohio Department of Agriculture, Division of Animal Helath:

1. Software Maintenance Agreement
2. Support and Problem Resolution Agreement

In addition, Ohio Department of Agriculture, Division of Animal Health can request additional enhancements where the cost and process are outlined in **Appendix A: Procuring Enhancements**.

A brief description of the deliverables and Pricing:

DESCRIPTION	COST
Software Maintenance Support and Problem Resolution SOW for **AgEnterprise with 50 support hours** **July 1, 2025 – June 30, 2026**	**$34,599.34**
Software Maintenance Support and Problem Resolution SOW for **AgEnterprise with 50 support hours** **July 1, 2026 – June 30, 2027**	**$36,575.00**

Additional support and enhancement hours may be purchased for **$120.00**/hour.

Support hours can be used for: Support, Training, Enhancement.

ACCLAIM is very pleased to support the Ohio Department of Agriculture, Division of Animal Health. If you have any questions, please contact:

John Kucek

johnku@acclaimsystems.com

773 495 8307

Software Maintenance

Software Maintenance is defined as the modification of a software product after delivery to correct defects and implement approved service requests, commonly referred to as 'break-fix." Services provide for resolution of any problems, defects, and/or deficiencies.

This contract is for the maintenance of AgEnterprise State Vet module.

What constitutes the use of maintenance hours?

Any request submitted to the service desk for investiagation, requested code change, requested reseach, emailed question with required response, 3rd party, request for participation in meetings, request for discussions with a 3rd party for services. Any request given from a client through the help desk.

Break-Fix

Under this Statement of Work (SOW), ACCLAIM will provide services to modify the **AgEnterprise** software in order to correct defects and implement approved service requests. If Acclaim Systems introduces a bug or break-fix error to the system through the normal release management process, Acclaim will remedy the issue. Existing unwanted features within the code that are deemed needing to be fixed will also be remedied within the current release management process at Acclaim Systems discretion. Unwanted features of the system that are as designed may or may not be fixed by Acclaim Systems and may require use of support hours to remedy.

Quality Assurance Process & Testing

ACCLAIM has several Quality Analysts at our development center in Harrisburg, PA.

ACCLAIM will test each major and minor release prior to delivery to the client in accordance with technical and business specifications agreed upon for the release, perform regression testing to validate that the new functionality has not negatively impacted existing functionality within the product, and provide the release for User Acceptance Testing (UAT). Clients are required to perform UAT during the time provided in the release management process. If UAT is not performed by the client, future unwanted features identified by the client may require support hours to remedy.

Release Deployment

ACCLAIM will provide a maintenance release schedule to the clients of AgEnterprise. Acclaim will work with the clients as much as possible to accommodate issues with the release:

- Standard releases: ACCLAIM will provide 1 standard release annually; This release can be pushed to each client, or a client can choose to skip one release. Acclaim systems will only support the current release and a prior release. If a client falls further behind, the cost for support will be impacted.

- Emergency release: Acclaim may provide up to 2 emergency releases during the year. Acclaim will exercise all commercially reasonable efforts to test such emergency fixes in accordance with the requirements of this section.

ACCLAIM also will deliver or make available to the client, with the delivery of each release, release notes describing the release content.

Release Management

Acclaim's Release Management process provides customer support, improved planning, and testing. This standardized approach to software delivery management provides for full quality assurance, communication, and consistency in versioning. Items to be included in a release are prioritized between our Product Management team and the clients. Acclaim will develop a maintenance release schedule, which will include any new modules identified by Acclaim and agreed-upon change requests through the support process.

Acclaim will provide support, as defined in this agreement, for the current major production release of the software and the current major production release – 1. Customers who choose to remain on older production release versions may be charged additional costs/hours for the added work effort in supporting older versions. Testing will be completed as much as possible, however, this may be greatly impacted with additional costs for the older the releases.

Product Management

Acclaim will provide product management to assist in coordination of support activities. As part of our maintenance service, our Product Manager, a subject matter expert in **AgEnterprise** will provide:

- Bimonthly (every other month) meeting to discuss the operations of **AgEnterprise** that focuses on:
    - Current support/training hour usage
    - Discussion of any new feature sets (enhancements) for changes that can be prioritized in a product release listing and product roadmap per a separate SOW
    - Shared discussion on other client activities or enhancement requests for prioritization
    - Discussion on internal infrastructure changes
- Coordinating with the client POC for prioritization and release dates of future releases

Product Management further includes:

- Providing information on enhancements or customizations made by other clients at no additional charge unless additional configurations are required to enable the functionality.
- Supporting User Group administration and meetings lead by the license holder of the software.
- Reviewing requested feature sets for prioritization across clients to be able to address high priority items as quickly as possible

- Assisting the user community in coordinating requirements, including potential cost sharing across clients
- User group conferences and user workshop coordination.

Client Responsibilities

This section describes the responsibilities of the client under this agreement.

- **Designated Support Contacts**

  The client will designate one (1) single point of contact (POC) with an optional backup. The POC is responsible for coordinating with the Acclaim Product Manager for prioritization and release dates of maintenance items as well as reporting and management of incidents.

  The client will designate one (1) or more product administrators to serve as the primary client contact for Acclaim's Support and Maintenance Services.

- **User Support**

  The client will provide end-user first-level support. Acclaim will provide and be responsible for Level 2 and 3 support of the product.`

- **Hosting (Production/Staging, Patch management, Backups and Procedures)**

  For products hosted by the client, the client will be responsible for:

  - Providing the Staging and Production Environments
  - Maintaining the staging and production environments
  - Performing all patch management and incident management in the environment
  - Performing all necessary back-ups, database monitoring and tuning, recovery, and required product operating procedures.
  - For products hosted by Acclaim, Acclaim will perform these tasks.

- **Remote Access**

  For products hosted by the client, the client will provide Acclaim remote access to the servers on which the product resides. For products hosted by Acclaim as an outsourced hosting service, the client will not have direct access, e.g., via virtual private network (VPN), to any of the hosted servers.

- **Client Assistance in Resolving Defects**

  The client will provide such assistance and cooperate with Acclaim in helping to identify and address defects. Providing full processes and procedures that were undertaken prior to and during the defect. Client delays in providing assistance affecting the total elapsed time of the maintenance task(s) related to the request may result in delayed completion of the task, charge of additional maintenance hours, or both.

  - When providing a detailed description of the issue you are experiencing, please remember to include such items and details as:

- User name experiencing the issue.
- Identify what the issue is exactly
- Identify what you expected to happen vs what happened.
- Document steps to reproduce issue.
- Identify the module/page - menu item selected to get to the page/report
- Parameters/data values populated, button clicked, etc.
- If any error message is displayed, please copy/include in the report.

Finally, be sure to select the appropriate Priority and click the Submit button.

Support and Problem Resolution Agreement

Support and Problem Resolution

The Acclaim Service Desk provides a single Point of Contact (PoC) for issue tracking and resolution for the Level 2 and Level 3 support requests. Acclaim provides SMEs on the **AgEnterprise** solution in conjunction with our Service Desk team to ensure a timely incident response and resolution to any issues or needs identified. Our Service Desk is available 8:00 a.m. to 7:00 p.m. Eastern Time on business workdays (No Holiday Coverage). Timeframes outside of these normal business hours are negotiable.

Additional details of support scope such as resolution times and issue resolution plan are provided in **Appendix C: Service Level Agreement**.

Product Contact Information

MODULE	EMAIL	TELEPHONE
AGENTERPRISE	AgEntrepriseState VetSupport@mail.acclaimsystems.com	(888) 999-2125

Figure 1: Solution Contact Information

Support Process

This agreement includes hours of support; these allocated hours of support will expire at the end of the contract term. Support hours include issue resolution for items outside of software Defects (i.e., data fixes), meetings to discuss software changes outside of Product Management monthly meetings, and enhancements or code changes, such as cosmetic changes on a report. Training includes webinars, continuing education training, and additional meetings to educate staff at the client request. Hours can be purchased should a client need additional support/training assistance. Support hours can be used for maintenance, enhancements and training.

Support and Maintenance Services History Tracking System

Acclim will maintain a customer- specific Support and Maintenance Services history, including updated records of the client's product configuration. Acclaim is committed to creating a transparent relationship and will log all of these support hours and classify them in the monthly statement:

a) the date, time, title and time spent on each contact to support desk

b) the total number of contracted hours, total used and remaining hours available.

Reporting and Management of Incidents

Reports of incidents (an "Incident Report") will be made by the client to the Acclaim Service Desk. If there are multiple Incidents, the client may prioritize their incidents with respect to each other. The Service Desk will log the reported incident and provide the client with an Incident tracking number for reference when making follow-up inquiries.

The Incident Report will contain:

a) the date and time of the call

b) the name of the product

c) the client contact name, e-mail address if available, and telephone number

d) a description of the incident

The client will provide Acclaim with as much information as possible to enable Acclaim to investigate and attempt to identify and verify the reported issue or defect. The client will work with Acclaim support personnel during the problem isolation process, as reasonably needed. Acclaim will manage and maintain records with respect to the resolution of all reported Incidents ("Incident Resolution Report") and may facilitate status calls for 'High Impact' or 'Work Stoppage' classifications. Acclaim will maintain the working history of Incident Reports and provide the client with expected resolution dates, and – for defects – a status of where the defect correction is in the Acclaim correction and quality assurance process.

Appendix A: Procuring Enhancements

For requested changes, Acclaim will draft a fixed-price SOW that details the scope, approach, assumptions and associated cost to meet the requested change. Acclaim's process for reviewing and estimating product enhancements/modifications is:

1. Client submits a work request to the Acclaim Support Desk through a support ticket.
2. The Acclaim Business Analyst working with other team members will outline a ball park estimate for this work. This ball park estimate will be sent through the help desk to the customer to see if they still want to move forward.
3. If the clients wants to move forward they will respond to the help desk with a go ahead.
4. The Acclaim Business Analyst then creates a detailed statement of work (SOW) that contains the documented requirements, assumptions, and cost. That SOW is delivered though the help desk to an authorized representative from the client for review and signature approval. The timing of this deliverable, in our experience, is dependent upon the scope and complexity of the requested enhancements.
5. Acclaim's team then places this detailed estimate into a product backlog item(s) and these are submitted for a future release of the application. The release chosen is based on the impact to the application and other clients. The PBI(s) will be worked on in the priority order and delivered through the release management process.

Appendix B: Terminology and Definitions

ACCLAIM's Quality Assurance Process includes:

- **Test Case Development** –Test cases are developed based on the acceptance criteria of the work to be delivered.These test cases cover both positive and negative test scenarios.
- **System Integration Testing (SIT)** – The objective of SIT is to verify the correctness of the newly designed items, and their interaction with the other functional areas of the system. Testing focuses on new or altered functionality of application.
- **Integration Testing (IT)** – The goal of IT is to logically combine all the key components described in the integration section of this document in strategic end-to-end testing flows to validate that all new functionality is processing correctly within the context of the entire system.
- **Regression Testing** – Regression Testing is done to confirm that a recent program or code change has not adversely affected existing production features. Regression Testing is a full or partial selection of previously executed test cases which are re-executed to ensure existing functionalities work to specification.
- **User Acceptance Testing (UAT)** – The client will test the application and sure that the software works as desired and expected after the release has been delivered into Staging. Once the client approves the release, the release is pushed to production. Any issues found during UAT will be addressed.

The following terms relating to Incidents and Defects are defined as follows:

- **Defect:** Any non-conformance of the Product to operate in accordance with the Documentation, or documented acceptance criteria that was introduced by features created by Acclaim Systems.
- **Emergency Release:** Corrections to a small number of known errors used to remediate a Major Incident and/or a potential security breach that might cause a Major Incident. Acclaim Inspection Services will follow the Emergency Change procedure and ensuing Emergency Release procedure to implement an Emergency Release for the impacted Customers.
- **Incident:** An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service.
- **Incident Response:** A email, and/or update from the Acclaim Service Desk or telephone call from Acclaim acknowledging that an Incident Report has been received and that appropriate technical personnel have been assigned to work on the Incident.
- **Interim Resolution:** Acclaim: (a) reinitiates or restarts, as applicable, the product, if the reported Defect caused the product to be inoperative; (b) enables the client to access the product, as applicable, if the reported Defect caused the client to be unable to access the product; or (c) provides the client with a workaround acceptable to the client that solves or mitigates a reported Defect.
- **Issue:** Any of the following: (a) any presently identified event, circumstance, or problem that adversely affects the ability to meet project requirements, or a missed Deliverable Due Date or Critical Milestone Due Date, whether by Acclaim or the client; or (b) any event, problem,

difficulty, or circumstance which affects or may affect the Product or the operation of the Product by the client, including the failure to meet the acceptance criteria. Issues do not include Defects (see definition of Defects).

- **Major Release:** Contains areas of new functionality, some of which may eliminate temporary fixes to problems. A major release usually supersedes all preceding minor releases and emergency releases. Acclaim Inspections Services must push a full (as opposed to partial) set of software components to the appropriate customer environment.
- **Minor Release:** Contains small enhancements and fixes, some of which may have already been issued as an emergency release. A minor release usually supersedes all preceding emergency releases.
- **Resolution:** A correction or modification that permanently corrects the Defect, or for non-Defect-based Incidents, a permanent product that ensures the Incident will not be repeated.
- **Service Request:** A request from a user for information, or advice, or for a Standard Change or for Access to an IT Service.
- **Work Stoppage:** Defined as a system Defect that directly impacts the daily operation of the business and provides no suitable work around.

Appendix C: Service Level Agreement

Resolution Times

The service is available 8:00 a.m. to 5:00 p.m. Eastern Time on Federal business days. Acclaim will respond within the timeframe noted in Figure 2. "Medium" and "Low" severity reported system defects and product deficiencies will be prioritized and corrected in a future product release.

		TIME TO:	
LEVEL OF SEVERITY	**DESCRIPTION**	**ACKNOWLEDGE**	**RESOLUTION PLAN**
1. High Impact	Software does not execute	1 hour	4 hours
2. Medium Impact	Software execution is significantly restricted or severely impaired		1 business day
3. Low Impact	Software executes with minor errors		5 business days

Figure 2: Resolution Times

Issue Resolution Plan

Client support is initially handled by Aclaim's Service Desk which will provide responsive and professional service for less complex support and will quickly transfer complex support needs to Acclaims Tier 3 team. Acclaim logs and tracks all problem contacts through resolution. Monthly reports to each client provide details on all calls and use of support time.

Technical support will be offered by telephone, email, and/or direct viewing of the production environment or mobile device. Acclaim requires direct access to client infrastructure (e.g., VPN) in order to execute this service agreement. Acclaim systems does not support the end user or the end users device.

As part of the Acclaim release management process, items will be prioritized between our Product Management team and the client. Acclaim will provide aging reports to review older support requests/bugs to ensure these items are being addressed as appropriate based on priority. All issues/bugs are reviewed prior to each minor release and targeted for a future release based on priority.

Acclaim's goal is to resolve all priority 1 items not considered for an emergency release in the next available release. Priority 2 items will be scheduled within the next two maintenance releases after submission to Acclaim. Any modifications to source code will follow standard release management for the specific product.

If you are impacted by a High Prority issue the process is to email the support desk, followed by a phone call to the Support Desk.

Escalation Procedures

Figure 3 describes the escalation path that is followed if the client escalates service requests and defects for which an Interim Resolution has not been provided and/or has not been addressed in a timely or appropriate manner. The client has the right to require Acclaim to assign an appropriate support and/or technical resource from Acclaim to coordinate and oversee resolution of such defect or request. In this case, resolution efforts will be communicated through daily calls. If these escalation procedures fail to produce a satisfactory resolution, the Executive Sponsors will discuss a corrective action plan to resolve the timeliness of correcting defects or requests.

Escalation Level	Contact Details
Lv. 1	AgraGuard Project Manager: Yda Mitzy G. Torres **Email**: mtorres@acclaimsystems.onmicrosoft.com
Lv. 2	Solution Account Manager: John Kucek **Email**: johnku@acclaimsystems.com **Phone**: (773) 495-8307
Lv. 3	Executive Director: David Burgess **Email**: Davidb@mail.AcclaimSystems.com

Figure 3: Escalation Path

Notice to Proceed

This Proposal dated April 22, 2025, for Acclaim Systems, Inc. (ACCLAIM) to provide Ohio Department of Agriculture, Division of Animal Health with services as described in the Software Maintenance Agreement, Support and Problem Resolution Agreement is hereby submitted for approval. The parties acknowledge that they have read this document, understand it, and agree to be bound by its terms and conditions.

This Notice to Proceed will serve an acceptance of this Proposal, as set forth in this document.

OHIO DEPARTMENT OF AGRICULTURE

By

Name

Title

Date

EXHIBIT B

DATA SECURITY AND PRIVACY TERMS

These Data Security and Privacy Terms ("Terms") describe the responsibilities for the Contractor relating to State information security and privacy standards and requirements for all proposed solutions, whether cloud, on-premises, or hybrid based. These Terms apply to all work, services, and personnel across all environments, and State of Ohio ("State") and Contractor locations (e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid) along with the computing elements that the Contractor will perform, provide, occupy, or utilize in performing the work, and any Contractor access to State resources in conjunction with the delivery of work.

The Contractor must comply with these Terms as they apply to the services being provided to the State. The Contractor is responsible for maintaining information security in any environments under the Contractor's management in accordance with these Terms.

These Terms are in addition to the Contract terms and conditions. In the event of a conflict between the Contract and these Terms, the most stringent standard will prevail.

Definitions

1. **Contract** means the contract entered into between the Contractor and the State to which these Terms are attached and/or incorporated.

2. **Contract Data** means State Data that the Contractor has access to, transmits, processes, possesses, creates or stores in providing services to the State.

3. **Contractor** means the person or entity with whom the State has entered into the Contract and, for purposes of these Terms, includes subcontractors or other personnel under the authority or control of the Contractor performing the work or providing the services under this Contract.

4. **Personally Identifiable Information** as defined in the Ohio Revised Code means information that can be used directly or in combination with other information to identify a particular individual. It includes:
   A. A name, identifying number, symbol, or other identifier assigned to a person,
   B. Any information that describes anything about a person,
   C. Any information that indicates actions done by or to a person,
   D. Any information that indicates that a person possesses certain personal characteristics.

5. **Security Event** is any observable occurrence that is relevant to information security within normal operational noise levels and below pre-defined incident thresholds that does not adversely impact or potentially impact Contract Data or information systems.

6. **Security Incident** means there is successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

7. **State Data** means all data and information provided by, created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Confidential Data. All State Data is and will remain the property of the State and, unless specifically provided otherwise in the Contract, Contractor acquires no right, title, or interest in or to State Data.

8. **Confidential Data** means any type of data that is required to be protected by law or regulation, is intended for confidential use, and may not be copied or removed from the State's operational control without authorized permission. Confidential Data includes data that, if compromised, may result in loss of life, serious injury, or other harm to an individual or group, or disruption to critical State operations. Confidential Data is included in the definition of Confidential Information in the Contract.

Confidential Data includes, but is not limited to:

A. Personally Identifiable Information (PII);
B. Student information under the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);
C. Federal Tax Information (FTI) under IRS Publication 1075 - Tax Information Security Guidelines for federal, state, and local agencies;
D. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164); United States Code 42 U.S.C. 1320d through 1320d-9 (HIPAA); and Code of Federal Regulations for Public Health and Public Welfare: 42 C.F.R. 431.300, 431.302, 431.305, 431.306, 435.945, 45 C.F.R. 164.502(e) and 164.504(e);
E. Criminal Justice Information (CJI) under the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy available at https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center;
F. Payment Card Industry Data Security Standards (PCI DSS);
G. Social Security Administration (SSA) Data which is data received by the State from the Social Security Administration in accordance with the current Computer Matching and Privacy Protection Act between the State of Ohio and the Social Security Administration; and
H. Other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

9. **State IT Security Policies and Standards** means the policies and standards available at https://das.ohio.gov/technology-and-strategy/information-security-privacy/information-security-governance.

Requirements

1. The Contractor's Responsibilities Generally

At a minimum, the Contractor must maintain the security of Contract Data in accordance with the moderate level security baseline of the current published version of the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," (NIST 800-53). In the alternative, the Contractor may maintain the security of Contract Data in accordance with International Organization for Standardization 27001 (ISO 27001) if the Contractor implements the additional necessary controls to achieve compliance with the requirements of NIST 800-53. Hereinafter, references in these Terms to "NIST 800-53" means both of the frameworks defined in this paragraph.

The Contractor must implement the information security policies, standards, and capabilities set forth in the Contract, support the State's adherence to the State IT Security Policies and Standards, and use procedures in a manner that does not diminish established State capabilities and standards.

If the Contractor accesses the State's facilities or networks, or provides products, solutions, or services that will be implemented or integrated in the State's controlled environment, the Contractor must ensure its products, solutions, or services comply with State IT Security Polices and Standards, as appropriate (available at the link provided above in the definition of State IT Security Policies and Standards).

The Contractor's information security and technology responsibilities with respect to the work and services the Contractor is providing to the State include the following, where applicable:

A. Assist in the implementation of associated security procedures with the State's review and approval, including physical access requirements, User ID approval procedures, and a Security Incident action and response plan.

B. Support implementation and compliance monitoring as per the State IT Security Policies and Standards.

C. Upon identification of a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.

2. Protection and Handling of Contract Data

The Contractor must maintain an information security program made up of policies, procedures, technical and organizational safeguards, and training designed to protect Contract Data against unauthorized loss, destruction, alteration, access, or disclosure. To protect Contract Data, the Contractor must use due diligence to ensure that computer and telecommunications systems and services involved in storing, using, or transmitting Contract Data are secure and prevent Contract Data from unauthorized disclosure, modification, use, or destruction. To accomplish this, the Contractor must adhere to the following requirements regarding Contract Data in addition to the confidentiality requirements in the Contract:

A. Assume all Contract Data is both confidential and critical for State operations.

B. Maintain, in confidence, Contract Data it may obtain, maintain, process, or otherwise receive from or through the State during the term of the Contract and pursuant to the provisions of the Contract and these Terms.

C. Use and permit its employees, officers, agents, and subcontractors to use any Contract Data received from the State solely to perform its obligations under the Contract.

D. Not sell, rent, lease, disclose, or permit its employees, officers, agents, and subcontractors to sell, rent, lease, or disclose, any Contract Data to any third party, except as permitted under the Contract or required by applicable law, regulation, or court order.

E. Take all commercially reasonable steps to (a) protect the confidentiality of Contract Data received from the State and (b) establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to Contract Data received by the Contractor from the State.

F. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of Contract Data.

G. Ensure that the Contractor's internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of Contract Data, and periodically review and update these policies, plans, and procedures as needed.

All Contract Data at rest in systems supporting the Contractor's services must reside within the contiguous United States with a minimum of two data center facilities at two different and distant geographic locations, ensuring physical and environmental protection controls are implemented as defined in State IT Security Policy 2100-15, and be handled in accordance with the requirements of these Terms at all Contractor locations. All Contract Data that is not classified as public by the State must be encrypted at rest and while in transit utilizing industry standards that meet Federal Information Processing Standards (FIPS) validated algorithms and comply with State IT Security Policy IT-14, Securing Confidential Data.

If the Contractor will be accessing, processing, transmitting, possessing, creating, or storing Confidential Data, the State may require additional documentation from the Contractor and/or input to complete State documentation.

3. Security Standards and Warranties

All solutions shall operate at the moderate level baseline as defined in the current published version of NIST 800-53, be consistent with Federal Information Security Management Act, 44 U.S.C. § 3551 et seq. (FISMA 2014) requirements and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications.

The Contractor's information security program must be designed to protect Contract Data by implementing an industry security and privacy standard including, at a minimum:

A. Security and confidentiality of Contract Data.

B. Protection against anticipated threats or hazards to the security or integrity of Contract Data.

C. Protection against unauthorized access to, disclosure of, or use of Contract Data.

D. Giving access to Contract Data only to those individual employees, officers, agents, and subcontractors who need to know such information in connection with the performance of the obligations under the Contract.

E. Cooperating with any attempt by the State to monitor compliance with the foregoing obligations as reasonably requested by the State.

F. Promptly destroying or returning to the State, in a format designated by the State, all Contract Data received from or through the State upon completion of the work under the Contract or upon termination or expiration of the Contract. Notwithstanding the foregoing, the Contractor may keep a copy of the Contract Data to comply with contractual, legal, or record keeping obligations, and any such retained Contract Data is subject to the requirements of this Contract for so long as the Contractor has the Contract Data in its possession.

G. Maintaining appropriate and effective business continuity and disaster recovery plans to ensure resiliency of Contract Data and business operations.

H. Maintain a privacy policy that includes, at a minimum, processes for the State to obtain individual privacy consent for the use of PII, at the determination of the State, and to respond to individuals' requests to access, correct, and delete their PII unless otherwise expressly agreed to in the Contract. All PII, including PII that has been de-identified, is considered Contract Data and Confidential Information under this Contract.

The Contractor must scan all source code for vulnerabilities, including before and after any source code changes are made, must promptly remediate vulnerabilities, and/or provide the State with patches to address the vulnerabilities at no cost to the State. The Contractor must follow best practices for application code review and the most current version of the Open Source Foundation for Application Security (OWASP) top 10.

In addition to the warranties provided and pursuant to the terms of the warranties section of the Contract (i.e., notification, correction, and indemnification), the Contractor warrants that its software is free from viruses, malware, and other harmful or malicious code.

4. Permitted Disclosure to Third Parties

Disclosure of Contract Data is permitted as set forth in the Contract. Additionally, disclosure of Contract Data is also permitted when required by applicable law, regulation, court order, or subpoena. If the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether Confidential Data or otherwise, pursuant to court or administrative order, subpoena,

summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule or regulation, the Contractor must notify the State within 24 hours of receipt of the order or request in order for the State to seek a protective order or take other appropriate action, as desired. The Contractor must also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State.

If, in the absence of a protective order, the Contractor is compelled as a matter of law to disclose the information provided by the State, the Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, the Contractor must advise and consult with the State and its counsel as to the scope of such disclosure and the nature of wording of such disclosure) and must use commercially reasonable efforts to obtain confidential treatment for the information disclosed.

The Contractor may disclose Confidential Information to the following people, subject to the requirements of the Contract and these Terms:

A. To State or Federal auditors or regulators.

B. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations.

C. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

5. Auditing

A. If the Contractor provides a solution, service, or product hosted by the Contractor or a cloud provider, the Contractor must obtain an annual audit of the services being provided under this Contract that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAE) No. 18, Service Organization Control 2 Type 2 (SOC 2 Type 2). At any point during the term of the Contract and if not already obtained, the Contractor may obtain and must thereafter maintain StateRAMP or FedRAMP authorization in lieu of a SOC 2 Type 2 audit.

B. If Contractor provides a solution, service, or product hosted by the Contractor or a cloud provider that completes a financial duty on behalf of the State, the Contractor must obtain an annual audit of the services being provided under this Contract that meets the AICPA SSAE No. 18, Service Organization Control 1 Type 2 (SOC 1 Type 2).

C. The SOC 1 Type 2 and SOC 2 Type 2 audits will be completed at the sole expense of the Contractor and the results must be provided to the State within 30 days of the Contractor's receipt of its audit results each year by emailing the results to Compliance@das.ohio.gov. The results of the audits provided to the State are considered Confidential Information under the Contract.

D. When required by law, rule, or regulation, or if the Contractor does not obtain or obtains an adverse opinion on the SOC 2 Type 2 audit described above, the State may, at any time in its sole discretion, elect to perform a security and data protection audit. This includes a thorough review of Contractor controls, security and privacy functions and procedures, data storage and encryption methods, and backup and restoration processes. The State may utilize a third-party contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met. The State will provide its request in writing and will work with the Contractor to schedule time to conduct the audit.

E. At no cost to the State, the Contractor must remedy material issues, material weaknesses, or other items identified in each audit as they pertain to the services provided under this Contract.

6. Background Investigations of Contractor Personnel

Any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (c) has been convicted of a felony may not perform certain services under the Contract.

The Contractor must conduct background investigations on Contractor personnel that may have access to Contract Data. The State may conduct background investigations on Contractor personnel that have or may have access to Confidential Data, critical infrastructure systems, or when required by law, rule, or regulation. The State will conduct initial background investigations on Contractor personnel who will have access to FTI and/or CJI that must be favorably adjudicated before being permitted to access the FTI and/or CJI, and ongoing background investigations every five years thereafter for personnel who already have access to FTI and/or CJI.

If any Contractor personnel refuses to have a background investigation completed or has an unfavorably adjudicated background investigation completed, the State may terminate that personnel's access to the Contract Data.

7. Security Incidents and Events

A. Categories

Security Incidents may fall into one or more of, but are not limited to, the following categories:

i. Loss or Theft
ii. Denial of Service (DoS)
iii. Improper Usage or Access
iv. Information Spillage
v. Malicious Code
vi. Phishing Messages
vii. Scans/Probes/Attempted Access
viii. Social Engineering
ix. Unauthorized Access

Security Events may fall into one or more of, but are not limited to, the following categories:

i. Unsuccessful log-on attempts
ii. Unsuccessful denial of service attacks
iii. Unsuccessful phishing attacks
iv. Unsuccessful network attacks such as pings, probes of firewalls, or port scans.

B. Security Incident Response and Reporting

The Contractor is responsible for Security Incident response, including containment, eradication, and recovery, to minimize the impact to the State. In addition to the requirements in the Contract, the Contractor must perform the following in response to a Security Incident involving Contract Data.

The Contractor is not required to report Security Events unless a pattern of attacks significantly increases the risk of impact.

The Contractor must report in writing to the State within 24 hours of the Contractor becoming aware of any Security Incident and/or use or disclosure of Contract Data not authorized by the Contract, including any reasonable belief that unauthorized access to or acquisition of Contract Data has occurred, and fully cooperate with the State to mitigate the consequences of the Security Incident.

Within five business days of the initial Security Incident report to the State, the Contractor must document and begin providing follow-up reports for all Security Incidents to the State. The Contractor must provide updates to the follow-up reports until the investigation is complete. At a minimum, the Security Incident reports will include:

i. Data elements involved, the extent of the Contract Data involved in the Security Incident, and the identification of affected individuals, if applicable.

ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed Contract Data, or to have been responsible for the Security Incident.

iii. A description of where the Contract Data is believed to have been improperly transmitted, sent, or utilized, if applicable.

iv. A description of the probable causes of the Security Incident and, in the final report, the root cause.

v. A description of the proposed plan for preventing similar future Security Incidents, including a recommended risk remediation plan.

vi. A description of the corrective actions taken, including repair (elimination of a defect or incident and/or restoration of system functionality requirements according to the Contract) and resolution (a temporary workaround to enable system function).

vii. Whether the Contractor believes any federal or state laws requiring notifications to individuals are triggered.

The Contractor must comply with all applicable laws that require the notification of individuals, or with other reasonable direction of the State for notification, in the event of a Security Incident involving personally identifiable information, or any other event requiring such notification. The State may, in its sole discretion, choose to provide notice to any or all parties affected by a Security Incident, but the Contractor shall reimburse the State for the cost of providing such notification. Contractor further agrees to provide, or to reimburse the State for its costs in providing, any credit monitoring or similar services that are necessary as a result of Contractor's Security Incident. Under Ohio law, Contract Data is State property and any illegal activity involving State property is subject to a criminal investigation. The Contractor shall preserve sufficient evidence to ensure accurate Security Incident records, facilitate an investigation, and determine the extent of the Security Incident.

The Contractor shall work with the State to establish a Security Incident reporting communications procedure including Contractor and State contacts, communication methods and tools. If there is no procedure established, the Contractor must report Security Incidents to the primary contact listed in the Contract or that contact's successor and the Contractor must report the Security Incident to the State via email at CSC@ohio.gov or call 877.644.6860.

The State reserves the right to conduct an independent investigation of the Security Incident, and the Contractor shall cooperate with the investigation. The independent investigation may be conducted by a State agency or a third party acting on behalf of the State.

8. Generative Artificial Intelligence

The Contractor must disclose the use of generative artificial intelligence (AI) to the State when producing work that will be owned by the State or the integration of generative AI in products or services used by the State. The Contractor must work with the State to ensure the use of generative AI is reviewed, approved, and complies with the State IT Policy IT-17, Use of Artificial Intelligence, prior to utilizing the generative AI

components. The Contractor is not permitted to utilize Confidential Data in training generative AI models except as specifically approved by the State.