CLOUD HOSTING APPENDIX

State of Illinois (State) Security Requirements:

1. Vendor will notify the State Chief Information Security Officer (CISO) within 24 hours of first becoming aware of any actual or reasonably suspected information breach or other security incident which impacts State data. Email notification must be sent to: DoIT.Security@illinois.gov with the subject line 'Breach Notification.' Vendor must provide an initial incident report within five (5) business days of the incident and a final incident report upon resolution. Reports must include a summary of the event, systems affected, root cause analysis, remediation steps, and any actions taken to prevent recurrence.
2. Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State with a security audit report, which shall be a System Operation Controls report (SOC 2 type 2), if available. Although the submission of such a security audit report is required, and the State strongly prefers the submission of a SOC 2 type 2 report to fulfill this requirement, the State in its discretion may agree to accept a similar, alternative type of security audit report for review, if no SOC 2 type 2 report is available. Vendor must provide a current report both at time of award and annually thereafter during the term of the Contract with applicable bridge/gap letter, or as soon as practical from an annual basis to the extent a new such report is then in the process of being prepared, or as otherwise may be agreed to by the State in its discretion.
3. Vendor must engage with the State's Third-Party Risk Management (TPRM) program, during onboarding and upon request, for risk assessment and monitoring purposes. This engagement includes timely responses to questionnaires, document submissions, and other actions required to evaluate and manage vendor risk.
4. Vendor must encrypt State data both at rest and in transit. This encryption must comply with encryption security controls as defined in the most current version of the Federal Information Processing Standard (FIPS) 140, using Advanced Encryption Standard (AES) encryption with a minimum key length of 256 bits. Vendor must provide proof of encryption. Vendor must provide the State with the capabilities to manage encryption keys for data at rest. These capabilities must not rely on a proprietary format or platform that prevents interoperability, visibility, or control by the State.
5. Vendor must only use State data for the purposes stated in this Contract.
6. Vendor may not use any State data in any non-production system or in any other system outside the application/service procured under this Contract. Vendor is strictly prohibited from using State data to train, fine-tune, or otherwise influence artificial intelligence or machine learning models, regardless of whether the data is anonymized or aggregated and regardless of whether such models are internal, external, open-source, commercial, experimental, or Vendor-operated.
7. No replication of State data to testing, development, sandbox, or non-production environments is permitted without prior written authorization from the State.
8. Vendor must provide a complete and current copy of all State data, in a non-proprietary, structured, and machine-readable format (e.g., JSON, XML, or CSV), without delay upon request by the State and upon termination of the Contract. Vendor must ensure that all metadata and file integrity are preserved. Vendor must assist in the secure transmission or migration of such data to an alternate State environment upon termination, at no additional cost to the State.

9. Vendor must ensure its system supports secure integration with the State Identity and Access Management (IAM) platform, including ILogin or any successor service designated by the Department of Innovation and Technology (DoIT), if credentialing is required for access to the system or its administrative functions. Integration shall apply to all interactive and administrative access and use industry-standard federated authentication protocols (e.g., SAML 2.0, OAuth 2.0, or OpenID Connect). Multifactor authentication (MFA) must be enforced for all privileged accounts. Vendor shall not create or maintain local user accounts for State personnel unless expressly authorized in writing by the State.
10. Vendor must provide a Software Bill of Materials (SBOM) for all products or services delivered under this Contract. The SBOM must identify all components, including open source and commercial libraries, versions, licenses, and known vulnerabilities. SBOMs shall follow a recognized format (e.g., SPDX, CycloneDX, or SWID), include dependency trees, and align with NTIA minimum elements. The SBOM must be updated with each major release or upon request by the State and made available to the State's designated vulnerability management repository.
11. Vendor must maintain a robust and reliable data backup system, with all backups encrypted using the same encryption standards defined in Section 4. Vendor must provide the State with a detailed description of its backup methodology, including backup frequency, storage location(s), retention schedules, and encryption processes. The backup methodology must meet all State-defined Maximum Tolerable Downtime (MTD) and Recovery Point Objective (RPO) requirements. Vendor must ensure backup integrity and demonstrate the ability to successfully restore data upon request.
12. At the State's request, Vendor must provide a written disaster recovery methodology and provide documented proof of annual disaster recovery testing. Testing documentation must include the test scope, methods used, results, issues discovered, and remediation plans. Vendor must maintain records of these tests for a minimum of three (3) years and make them available to the State upon request.
13. Vendor must sanitize all media that contains or contained State data using the most current revision of NIST Special Publication 800-88 (Guidelines for Media Sanitization). Vendor must certify in writing the sanitization method used, date and time of sanitization, and identification of the media sanitized. Certification must be signed by an authorized representative of the Vendor.
14. Vendor must render all State data hosted within its environment permanently inaccessible using crypto shredding or equivalent cryptographic sanitization methods approved by the State. Vendor must certify the successful completion of this process in writing and provide metadata or logs validating data destruction, upon request.
15. Vendor and/or its agents must not resell nor otherwise redistribute information gained from its access to the State data.
16. Vendor must not engage in, nor permit its agents to engage in, the delivery, installation, or activation of adware, unauthorized software, or any form of marketing, telemetry, or user tracking features unless explicitly authorized in writing by the State.
17. Vendor shall have a documented security incident policy and plan. Vendor must supply a copy at the request of the State. Vendor shall provide documented proof of annual testing of the plan. Vendor must notify the State of any material changes to the plan within 30 days.
18. Vendor must comply with all United States federal and State of Illinois laws, rules, and regulations. Vendor must cooperate fully with any federal or State audit or security review related to the systems, services, or data covered by this Contract.

19. Vendor must comply with all of the State's Enterprise Security Policies (https://doit.illinois.gov/initiatives/cybersecurity/policies.html.)
20. Vendor program and project management personnel must ensure coordination of activities with the State governance program. Vendor must comply with all policies, standards, and procedures defined by DoIT's Enterprise Portfolio Management Office.
21. When hosting or processing State financial information, Vendor must provide an SSAE-18 SOC 1 Type 2 report annually, along with any applicable bridge or gap letters. Reports must cover the full audit period and describe controls relevant to financial data handling, segregation of duties, and fraud prevention. Reports must be provided upon contract award and annually thereafter. All SOC reports must cover a period not exceeding twelve (12) months prior to the date of submission.
22. Vendor must ensure that all information technology products, services, and digital content provided under this Contract comply with the Illinois Information Technology Accessibility Act (30 ILCS 587) and the IITAA 2.0 Standards, which incorporate the Revised Section 508 Standards and the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. Accessibility compliance must be maintained throughout the system lifecycle, including during updates, upgrades, and new releases, and any material changes that affect accessibility must be remediated or mitigated in coordination with the State.
23. Vendor's system must meet the general requirements set forth in the State's Minimum Logging Requirements (Appendix S1).
24. Vendor's system must log activity in accordance with the State's Minimum Logging Requirements (Appendix S1) for the term of the Contract. Vendor must provide logs within 24 hours of request from the State in a JSON, CSV, or other acceptable to the State format.

Appendix S1 — Minimum Logging Requirements

1. Input and Output Validation Events

1.1 The system shall log all input validation failures, including protocol violations, unacceptable encodings, malformed data, and invalid or out-of-range parameters.
1.2 The system shall log all output validation failures, including unexpected data structures, encoding mismatches, data type errors, or inconsistent record sets.

2. Authentication and Access Control

2.1 The system shall log all authentication attempts, including successes, failures, account lockouts, MFA challenges, and MFA failures.
2.2 The system shall log all authorization failures (i.e. failed MFA, wrong password, account lockout, account disabled, etc.) and denied access attempts to protected resources or functions.
2.3 The system shall log all session management events, including session creation, termination, timeout, token anomalies, and any modification of session identifiers.
2.4 The system shall log all password reset actions including, but not limited to reset requests, reset completions, and failed reset attempts.
2.5 The system shall log all security related profile changes including, but not limited to MFA device added or remove, update to MFA type, MFA reset actions, and MFA type addition or change.

3. System and Application Events

3.1 The system shall log all application errors and exceptions, including syntax, logic, runtime, and unhandled errors.
3.2 The system shall log connectivity issues, third-party service failures, and file system errors.
3.3 The system shall log all virus or malware detections, blocked file uploads, and quarantine actions.
3.4 The system shall log all configuration changes to system, application, or security settings.
3.5 The system shall log all system and application startup, shutdown, restart, and logging service initialization events (start, stop, or pause).

4. Privileged and Administrative Activity

4.1 The system shall log all use of administrative or elevated privileges.
4.2 The system shall log the creation, modification, disabling, or deletion of user accounts or groups.
4.3 The system shall log changes to privileges, roles, tokens, access rights, or identity mappings.
4.4 The system shall log the use of system-level administrative functions, command execution, and high-risk application actions.
4.5 The system shall log access to or use of data-encrypting keys, including key creation, rotation, and destruction.
4.6 The system shall log the creation or deletion of system-level objects, datasets, or protected configuration files.

5. Data Access and High-Risk Operations

5.1 The system shall log all access to sensitive or regulated State data, including financial, personal, or cardholder data.

5.2 The system shall log all data import, export, bulk transfer, or generation of system-level reports.

5.3 The system shall log all submission or upload of user-generated content, including files or attachments.

5.4 The system shall log application-initiated network connections or outbound data transmissions.

6. Legal and Consent Events

6.1 The system shall log acceptance of terms of use, privacy notices, data usage statements, disclaimers, or other legal agreements.

6.2 The system shall log all user opt-ins or consent for mobile device capabilities, personal data usage, marketing communications, or other regulated actions.

General Requirements

7. Timestamping

7.1 All logs shall include accurate timestamps synchronized to a reliable time source (e.g., NTP).

7.2 All timestamps shall use a consistent time standard across all systems.

8. Log Integrity

8.1 Logs shall be protected against unauthorized modification or deletion.

8.2 The system shall generate integrity controls (e.g., hashing, checksums) to detect tampering.

9. Correlation

9.1 Logs shall contain sufficient detail to support event reconstruction, including at minimum: user or service account ID, session ID, source IP address, event type, resource accessed, and action taken.

10. Retention

10.1 Logs shall be retained in accordance with the State's Enterprise Security Policies and applicable laws or regulations.

10.2 Archived logs shall remain accessible to the State upon request.

11. Availability and Access

11.1 Logs shall be made available to the State upon request for audits, investigations, or security reviews.

11.2 When required, the system shall support secure log forwarding to the State's SIEM.