State of Illinois Standard Security Requirements

1. An information security risk assessment, data classification and system categorization process, and the submission of a system security plan must be completed and submitted to the Department of Innovation and Technology, Division of Information Security prior to the commencement of system development or solution delivery activities. Vendor must participate with the risk assessment and data classification and system categorization process. The formal risk assessment and data classification and system categorization process will be administered by the Illinois Department of Innovation and Technology, Division of Information Security. Vendor program and project management personnel must ensure the coordination of these activities with State of Illinois program and project management personnel.

   If not specifically addressed in other Vendor Information Technology Requirements, Vendor must adhere to State of Illinois technology and security Policies, Procedures, and Standards (https://doit.illinois.gov/initiatives/cybersecurity/policies.html).

   Vendor must also adhere to a minimum security baseline as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Systems and Organizations (https://doi.org/10.6028/NIST.SP.800-53r5, or as most recently updated). If not specifically addressed in other Vendor Information Technology Requirements, Vendors must assure the adoption of, at minimum, the low security control baselines. Exceptions to this requirement must be approved by the Illinois Department of Innovation and Technology, Division of Information Security.

   Cloud solutions must adhere to recommendations of the Cloud Security Alliance. Vendors may find guidance and cross-referencing to the NIST 800-53, Revision 5, or as most recently updated with the Cloud Security Alliance controls at CSA (cloudsecurityalliance.org).

   Throughout the term of this Contract, Vendor shall supply a current list of all non-proprietary/open-source software used in their solution. Vendor must also include the version and Open Source Initiative (OSI) approved license type used for any open source software. If Open Source uses non-OSI approved licensing Vendor must include and provide licensing terms and conditions for State review.

Vendor shall ensure any products, subscriptions, and/or services made available under this Contract will interface with the State's identity and access management solutions if authentication is required for access to the system.

Vendor shall ensure any products, subscriptions, and/or services will log activity in accordance with the State's Minimum Logging Requirements (Appendix S1) for the term of the Contract.

Vendor shall obtain and provide logs within 24 hours of request from State of Illinois in a non-proprietary, readily usable format.

Vendor shall ensure remediation begins within 24 hours of discovery for all critical and high (CVSS 7.0 and higher) vulnerabilities, as well as any additional vulnerabilities as determined by the State of Illinois.

Vendor must provide notice to the State of Illinois within 24 hours of the discovery of any critical and high (CVSS 7.0 and higher) vulnerabilities.

State and Federal laws, rules, and regulations as well as industry-specific guidelines require specific and often enhanced security controls on information and systems. The State of Illinois is required to comply with the below laws, standards, and regulations. Vendors must ensure compliance with the below as appropriate based upon the formal risk assessment to include a data classification and system categorization process.

- Illinois Identity Protection Act (5 ILCS 179)
- Illinois Personal Information Protection Act (815 ILCS 530)
- The Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99)
- Federal Bureau of Investigations Criminal Justice Information Services ("CJIS") Security Policy, version 5.5, issued June 26, 2016
- Federal Centers for Medicare & Medicaid Services ("CMS") MARS-E Document Suite, Version 2.0 Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges November 10, 2015.
- Federal Centers for Medicare & Medicaid Services Information Security Acceptable Risk Safeguards ("ARS") CMS Minimum Security Requirements Version 2.0 September 20, 2013.

2. Data Center Location and Access:
    a. Data Center Location: The physical location of any data center utilized by Vendor, made available, or used by any products, services, and

subscriptions under this Contract where State Data (as defined in Section 4.33 of this Contract) is stored or processed shall be within the contiguous United States, unless otherwise specifically agreed in advance by the State in writing at any time throughout the duration of the Contract.

b. Data Access: Vendor as well as any product, service, and subscription made available under this Contract shall only transmit, receive, process, or access State data that contains confidential, sensitive, or personal information: (i) to the extent permitted by the State under this Contract; and (ii) then only within the contiguous United States, unless otherwise specifically agreed in advance by the State in writing at any time throughout the duration of the Contract.

3. Data Use: Use of any data provided by the State, generated in the course of performing services under this Contract, or otherwise obtained from the State (collectively "State Data"), whether by Vendor or any product, service, or subscription made available under this Contract, is strictly limited to fulfilling its obligations under this Contract and for no other purpose without the prior written consent of the State. State Data does not include Vendor's proprietary data or information developed independently without reference to State Data. All other use of State Data, including but not limited to sharing, selling, or utilizing State Data for purposes not otherwise explicitly stated in this Contract, is expressly forbidden.

4. Permitted Use of Artificial Intelligence (AI): Vendor and any product, service or subscription made available under this Contract shall not utilize any Artificial Intelligence (“AI”) system, model, tool, or functionality in the performance of its obligations under this Contract, including the development, delivery, support, or the modification, upgrade, or enhancement of any product, service, or deliverable, or any component thereof, provided under this Contract (“AI Use”), except where such AI Use is both expressly: (i) disclosed to the State by Vendor and (ii) specifically authorized in writing by the State. For the avoidance of doubt, no AI Use shall be inferred or implied as permitted under this Agreement; all permitted uses must be expressly and specifically stated herein.
    a. Additional Limitation: Subject to the other restrictions herein, any State authorization provided for AI Use shall be strictly limited to the scope and purposes described in this Contract. Vendor shall not expand or modify its AI Use in any material respect beyond any existing State authorization provided without the prior written consent of the State, and such consent shall be subject to applicable law, rule, regulation, and policy.

b. Notice Requirement: Vendor shall promptly notify the State in writing of any material change in the AI systems used, including but not limited to version changes, shifts in model architecture, or changes in training data sources. Vendor shall provide prompt written notice to the State in the event any product, service, or subscription made available under this Contract adopts the use of AI in whole or in part.

5. Disclosure of Permitted AI Use: Vendor shall disclose, or shall otherwise ensure the disclosure of, the nature and extent of AI contributions and involvement in relation to any and all permitted uses of AI under this Contract ("AI Disclosures"). AI Disclosures must be provided in a clear, prominent, and contextually appropriate manner.
    a. Real-Time User Interface Disclosure: AI systems that contain a user interface must clearly identify the interaction as AI-driven, state the model's name as well as its role and limits, and provide a conspicuous on-screen link or control for deeper detail.
    b. Backend or Embedded AI Functionality: Where AI systems made available under this Contract lack a direct user interface, Vendor ensure shall ensure AI Disclosures are provided to the relevant end-user or product owner prior to purchase.
    c. AI-Generated Output Labelling: All deliverables and content wholly or partly produced by AI or derived from AI generated content shall be unmistakably marked in a contextually appropriate manner as determined by the State so the State and users can readily distinguish such content from purely human-authored content.

6. Legal Compliance of AI: Vendor shall ensure that all deliverables, products, subscriptions, services, or content that that are themselves AI, or embed AI, or rely on AI provided under this Contract are compliant with applicable law.