

ATTACHMENT L: FIRST AMENDED AND RESTATED MINIMUM INFORMATION SECURITY REQUIREMENTS

1. Definitions.

The following definitions apply to this attachment.

- a) "Data Policy" means the Statewide Data Classification and Handling Policy located at <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.
- b) "Agreement" means the executed contract for goods or services between the State of North Carolina and Vendor, including all exhibits, attachments, schedules, statements of work, service level agreements, amendments, and documents or policies incorporated by reference, that collectively govern the rights, obligations, and responsibilities of the parties.
- c) "Generative Artificial Intelligence ("GenAI"): any machine learning, deep learning, neural network, large language model, diffusion model, transformer-based model, or other artificial intelligence system that is trained on data to autonomously or semi-autonomously generate, synthesize, predict, modify, or transform text, images, audio, video, software code, data, analyses, or other content in response to prompts, inputs, queries, or other stimuli, including systems that continuously learn or are fine-tuned using additional data.
- d) "Information Technology Services" ("IT Services" or "Vendor's Systems") refers to any systems, applications or platforms operated, managed, or utilized by Vendor, its agents, or Subcontractors, that access, process, store, transmit, or otherwise handle State Data, including, without limitation, any cloud-based or on-premises Solutions associated with the provision of their services.
- e) "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors associated with their services.
- f) "Processing" means any operation or set of operations performed upon the State Data, whether by automatic means such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) "Security Breach" under the North Carolina Identity Theft Protection Act (N.C.G.S. § 75-60 et seq.), means:
 - i. Any circumstance pursuant to which applicable Law requires notification of such breach to be provided to affected parties or requires other activity in response to such circumstance (including, without limitation, N.C.G.S. § 75-65); **or**
 - ii. Any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Vendor's Systems Security in a manner that does or could reasonably be expected to permit the unauthorized Processing, use, disclosure, acquisition of, or access to any of the State's Data or Restricted State Data or Information.
- h) "Security Incident" means any actual or suspected event that:
 - i. Compromises, or disrupts access to or the use of, the State's Data or Vendor's Systems;
 - ii. Involves fraudulent activity related to or affecting the State's Data or Vendor's Systems;
 - iii. Results in the introduction of malware, viruses, or disabling devices into the State's Data or Vendor's Systems; **or**
 - iv. Results in the loss, corruption, unauthorized disclosure of, or unauthorized access to, the State's Data or Vendor's Systems.

Exclusions

The following events shall not, by themselves, constitute a Security Incident under this agreement, provided that such events do not result in an actual compromise of security and remain within normal operational thresholds:

- i. Unsuccessful attempts to log into a system or database using invalid credentials;
- ii. Denial-of-service attempts that do not materially degrade, disrupt, or interrupt service or result in a system being taken offline;
- iii. Routine network activity, including firewall pings;

- iv. Port scans; and
 - v. Worms, viruses, and other malware.
- i) **“Restricted State Data”** means any non-public data that is classified by the State of North Carolina, now or in the future, as restricted or highly restricted under the Statewide Data Classification and Handling Policy (Data Policy) or applicable law, including personally identifiable information and any other data that requires enhanced safeguards to protect its confidentiality, integrity, or availability.
 - j) **“Security of ‘IT Services’ or ‘Vendor’s Systems’”** means the security, integrity, and protection of any computer, electronic, or telecommunications systems of any kind, including, without limitation, applications, databases, hardware, software, storage, and networking components (including switching and interconnection devices and mechanisms), together with any networks of which such systems are a part or with which they communicate, that are used directly or indirectly by Vendor or its agents or subcontractors associated with their services.
 - k) **“State Data”** means all information created, received, stored, processed, or transmitted by or on behalf of a state agency as part of official State business — regardless of format, system, or who ultimately holds it
 - l) The **“State”** means the State of North Carolina acting through the North Carolina State Health Plan for Teachers and State Employees ("Plan") or, as determined by the Plan, the North Carolina Department of Information Technology or other State Agency.
 - m) **“Vendor”** means any entity contracted by the State to provide goods or services under a formal, executed Agreement, **including, without limitation, legal Firms and other professional service providers**. This term includes not only the primary contracting party, but also any of its agents, representatives, or subcontractors who, in the course of fulfilling the Agreement, may access, process, store, transmit, or otherwise handle the State’s Data.

2. **Conflict of Terms.**

In the case of a conflict between specific provisions of Attachment L and the Parties’ Business Associate Agreement (BAA) regarding any State data that is not PHI, Attachment L shall control to the extent of a conflict. In the case of a conflict between specific provisions of Attachment L and the Business Associate Agreement regarding State Data that is PHI, or any other information that is PHI, the Business Associate Agreement shall control to the extent of the conflict and allow for compliance with HIPAA and HITECH.

3. **Protection of the State’s Restricted Data.**

Vendor acknowledges its responsibility to secure all Restricted State Data, as defined by the Data Policy located at <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

Vendor warrants, at its sole cost and expense, that it shall:

- a) Implement appropriate processes and controls to maintain the security of Restricted State Data;
- b) Exercise reasonable care and diligence to detect any fraudulent activity involving such data; and
- c) Promptly notify the State of any confirmed Security Breach as soon as practicable, but no later than twenty-four (24) hours after confirmation, or within such shorter timeframe as may be required by N.C.G.S. § 143B-1379.

4. **Storing State Data outside of the United States.**

Vendor shall not store or transfer Restricted State Data outside of the United States. This includes backup data and Disaster Recovery locations.

5. **State Data and Service Safeguards.**

Vendor shall implement all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of this Agreement to secure State Data from Data Breach, and protect it and all IT Services associated with the provision of their services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State’s access to its data and their services.

6. Encryption of Restricted State Data.

Vendor shall encrypt all Restricted State Data while in transit, regardless of the transmission method or transport mechanism used. Additionally, vendors storing Restricted State Data shall ensure that such data is encrypted at rest. All encryption mechanisms used by Vendor must employ cryptographic modules validated in accordance with the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*.

7. Breach Notification.

- a) In the event Vendor becomes aware of any Security Breach caused by an external unauthorized individual or group, or acts or omissions of Vendor other than in accordance with the terms of the Agreement, Vendor shall, at its own expense:
- i. Immediately notify the State's Contract Administrator of such Security Breach and perform a root cause analysis thereon;
 - ii. Investigate such Security Breach;
 - iii. Provide a remediation state, acceptable to the State, to address the Security Breach and prevent any further incidents;
 - iv. Conduct a forensic investigation to determine what systems, data and information have been affected by such events;
 - v. Cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach.
- b) The State shall make the final decision on notifying the impacted people, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation state.
- c) If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all people and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required;
- d) The State retains primary authority over Incident Response, and Vendor bears associated costs caused by Vendor's acts or omissions;
- e) Vendor shall indemnify and hold harmless the State for claims arising from Security Incidents or noncompliance.

8. Security Logging and Availability.

Vendor shall maintain security logs sufficient to support audit, forensic investigation, and incident response activities related to the State's Data and their services. Such logs shall be retained for a minimum of twelve (12) months, unless otherwise required by law or agreed in writing by the State. Vendor shall make relevant security logs available to the State upon request, in a reasonable and usable format, solely for the purpose of security review, audit, or incident investigation. Nothing in this provision shall be construed to require Vendor to provide continuous or direct system access to the State.

9. Notification Related Costs.

Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or associated with any Security Breach due to acts or omissions of Vendor other than in accordance with the terms of this Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach including, but not limited to

- a) Preparation and mailing or other transmission of legally required notifications;
- b) Preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate;
- c) Establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training);
- d) Public relations and other similar crisis management services;
- e) Legal and accounting fees and expenses associated with the State's investigation of and response to such events; and

- f) Costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances.

If Vendor becomes aware of any Security Breach which is not due to acts or omissions of Vendor other than in accordance with the terms of this Agreement, Vendor shall immediately notify the State of such Security Breach and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable charges for the same.

10. Notice of Data Movement.

During normal operations, Vendor may need to copy or move State Data to another storage location within Vendor's Systems and delete the State Data from its original location. In any such event, Vendor shall preserve the content, integrity, and confidentiality of the State Data during and after such transfer.

Except as required for routine operational processes, Vendor shall not materially alter, relocate, or delete State Data without providing prior written notice to, and obtaining prior written approval from, the State.

11. Accessing State Data from Outside United States.

Remote access to State Data from outside the continental United States including, without limitation, remote access to State Data by authorized services support staff in identified support centers, is prohibited unless approved in advance by the State or designee of the State in writing.

12. Vendor's Systems Loss and Restoration.

In the event of temporary loss of access to services, Vendor shall promptly restore continuity of services, restore State Data in accordance with this Agreement and as may be set forth in a Service Level Agreement (SLA), restore accessibility of State Data and their services to meet the performance requirements stated herein or in an SLA. As a result, service level remedies will become available to the State as provided herein, in the SLA, or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.

13. Disaster or Catastrophic Failure.

In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data or IT Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State or designee of the State. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:

- a) The scale and quantity of the State Data loss;
- b) What Vendor has done or will do to recover the State Data from backups and mitigate any adverse effect of the State Data and services loss; and
- c) What corrective action Vendor has taken or will take to prevent future State Data and services loss;
- d) If Vendor fails to respond immediately to remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement;
- e) Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation.

14. Return of State Data.

In the event of termination of this Agreement, cessation of business by Vendor, or other event preventing Vendor from continuing to provide their services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, and shall promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so and on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. Vendor shall also provide the State with any data maps, documentation, software, or other materials necessary including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

15. Secure Data Disposal.

When requested by the State, Vendor shall destroy all requested State Data in all its forms (e.g., disk, digital tapes, CD/DVD, and paper). State Data shall be permanently deleted and shall not be recoverable according to National Institute of Standards and Technology (NIST), approved methods and certificates of destruction shall be provided to the State. Upon the expiration or termination of this Agreement, or upon written request by the State, Vendor shall return State Data and certify secure destruction within 30 days in a State-approved format and securely destroy all remaining copies, including backups, in accordance with NIST-approved destruction methods.

16. Security Risk and Compliance Assessment.

North Carolina's Statewide Information Security Policies provide the framework for safeguarding information technology assets across the state. These policies establish the security standards mandated by N.C.G.S. §143B-1376, which assigns the State Chief Information Officer responsibility for creating statewide IT Security standards to enhance the functionality, security, and interoperability of the State's assets. These policies apply to all assets, i.e., State Data and Vendor's Systems, whether managed directly by the State or by contractors and other organizations acting on its behalf. Authorization to use systems that store, process, or transmit State restricted information is strictly controlled to ensure that only approved systems are utilized.

To support compliance with the State security standards and enable the State's assessment of IT Services and State Data related to risk and compliance, all vendors are required to provide the State with a complete inventory of the IT Services associated with the provision of their services. This requirement ensures that all IT services, whether new, existing, or being renewed, are fully and accurately documented and evaluated for security risk and compliance. Accordingly, Vendors must ensure that all information related to IT services is accurate and up to date.

a) Vendor Compliance:

- i. Vendor shall submit all requested security documentation. The submitted materials will be reviewed by the State to determine whether the system meets applicable State security requirements prior to award.
- ii. Compliance with the requirements set forth in this Agreement is a material condition of the Agreement. Any failure by Vendor to comply with the security, privacy, data protection, or system control obligations identified in this Agreement shall constitute a material breach of the Agreement.
- iii. Upon identification of noncompliance, the State reserves the right, in its sole discretion, to take appropriate enforcement actions, which may include requiring corrective action plans; temporarily suspending access to systems, data, or services; withholding payment; or terminating this Agreement in whole or in part. Such actions may be taken without limiting any other rights or remedies available under the Agreement, at law, or in equity.
- iv. Termination or suspension under this provision may occur immediately when the noncompliance poses a risk to the confidentiality, integrity, or availability of systems or State Data, or where Vendor fails to timely remediate identified deficiencies. Vendor shall remain responsible for all obligations that, by their nature, survive termination, including but not limited to data protection, confidentiality, audit cooperation, and incident response obligations.

- v. Vendor shall ensure that all subcontractors, agents, affiliates, or third parties engaged to perform any portion of their services are contractually bound to security and data protection obligations no less stringent than those set forth in this Agreement.
- vi. Vendor remains fully responsible and liable for the acts, omissions, and compliance of its subcontractors as if such acts or omissions were those of the Vendor itself. The use of subcontractors shall not relieve Vendor of any obligations under this Agreement, including compliance with applicable security standards, audit requirements, incident notification timelines, or data handling restrictions.
- vii. Vendor shall not engage any subcontractor that materially impacts system security or data processing without prior disclosure, and as required by this RFP, prior written approval. Upon request, Vendor shall provide documentation demonstrating that subcontractors are subject to appropriate contractual security controls, including but not limited to security addenda, flow-down clauses, or equivalent written assurances.
- viii. The State understands that security assessment reports and security information provided to the Plan for the purpose of this Agreement may contain confidential information and/or trade secrets.

b) Vendor's IT Services Security Assessment Material:

Vendor shall provide the North Carolina State Health Plan (Plan) the following Information Technology security materials :

- i. Identify all systems, applications or platforms (whether cloud-based or on-premises) to be used by the Vendor, its agents, or subcontractors to provide the services under this RFP that access, collect, store, process, transmit, or otherwise handle State Restricted Data. For each system, Vendor shall provide the following:
 - 1) Service name;
 - 2) Service provider;
 - 3) Service administrator;
 - 4) Service hosting organization;
 - 5) Internet address (if applicable);
 - 6) Primary function of the Service;
 - 7) Whether the service utilizes Generative AI (Yes/No);
 - 8) Whether data resides exclusively within the United States (Yes/No);
 - 9) Type of third-party security attestation (e.g., SOC 2, GovRamp, HITRUST); and
 - 10) An un-Redacted copy of the corresponding third-party assessment report.
 - ii. Vendor shall provide a valid and favorable independent third-party assessment report on all related security controls that are consistent with, and can be cross walked to, the data classification level and security controls appropriate for moderate information system(s) per the National Institute of Standards and Technology ("NIST") SP 800-53 Rev. 5 or the most recent revision. To satisfy this requirement, such reports must have been issued within twelve (12) months prior to the anticipated Contract award date or be supplemented by bridge letters covering no more than three months after the report expiration date. Vendor hereby agrees that the Plan has the right to independently evaluate, audit, and verify such requirements as part of its continuous assessment and during the life of the Contract. The Plan will verify any such third-party security opinions or attestations yearly during the life of the Contract, and Vendor will be required to timely provide an updated report or bridge letter verifying that there have been no material changes in the Scope of the Examination reported since the issuance of the last report.
- c) Additional Security Documentation: Prior to Contract award, the Plan may in its discretion require Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor shall provide additional security documentation upon request by the Plan during the term of the Contract.
- d) The Plan understands that security assessment reports and security information provided to the Plan for the purpose of this RFP may contain confidential information and/or trade secrets. Refer to Section V, Paragraph 24

“Confidential Information” of Attachment B: Instructions to Vendors for information regarding the treatment of Confidential Information.

17. Use and Disclosure of GenAI During the Term of the Agreement.

- a) During the term of the Agreement, Vendor must promptly notify the State in writing if Vendor’s Services or any work under this Agreement includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors.
- b) Vendor shall not activate such GenAI technology without the State’s written consent and approval.
- c) The State may, in its sole discretion, require Vendor to provide additional information for Vendor’s GENAI technology related to privacy, security, and architecture.
- d) Failure to disclose GenAI use to the State may be considered a breach of the Contract by the State at its sole discretion. The State may consider such failure to disclose GenAI or any failure to provide requested information related to privacy, security, or architecture, as grounds for the immediate termination of the Agreement. The State is entitled to seek any and all relief it may be entitled to as a result of Vendor’s failure to disclose GENAI.
- e) The State reserves the right to incorporate GenAI Special Provisions into this Agreement at the State’s sole discretion and/or terminate any Agreement that presents an unacceptable level of risk to the State.

18. Information Security Program.

Vendor shall maintain Information Security Program that addresses, and during the term of this Agreement shall address, the following areas: (i) Access Control; (ii) Awareness and Training; (iii) Audit and Accountability; (iv) Assessment, Authorization, and Monitoring; (v) Configuration Management; (vi) Contingency Planning; (vii) Identification and Authentication; (ix) Incident Response; (x) Maintenance; (xi) Media Protection; (xii) Physical and Environmental Protection; (xiii) Planning: (Program Management: (xiv) Personnel Security; (xv) Risk Assessment; (xvi) System and Services: (xviii) Acquisition: (xix) System and Communications Protection: (xx) System and Information Integrity; (xxi) Supply Chain Risk Management; (xxii) Personally Identifiable Information Processing and Transparency.

19. Compliance with Laws and Standards.

Vendor certifies that it shall treat the State’s property and State Data in compliance with legal requirements and applicable industry standards with respect to privacy and State Data security, including without limitation any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377; Privacy provisions of the Federal Privacy Act of 1974; The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66); The North Carolina Public Records Act, N.C.G.S. Chapter 132; and Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA); Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.

20. Survival.

The provisions of this exhibit shall survive the termination or expiration of this Agreement for as long as Vendor or its Subcontractor has possession of or access to the State’s materials.