GENERAL CONDITIONS OF PURCHASE
ADDENDUM B – Information Technology Requirements

1. Division of Enterprise Technology Strategy and Services ("ETSS") Policies & General Applicability

(a) All ETSS policies applicable and in effect as of the contract execution date are set forth in Exhibit 1 – IT Policies. ETSS policies may be located using the link: Enterprise Policies. Policies are reviewed and updated annually or upon major revision.

(b) Notwithstanding the applicability of the policies referenced above, should any portions of the ETSS Policies and this Addendum B conflict, Addendum B takes precedence and controls.

(c) The provisions of this Addendum B apply to every contract to which the State is a party, unless expressly agreed otherwise by the State.

2. ETSS Security Questionnaire

(a) Any ETSS Security Questionnaire, the Vendor's response to such Security Questionnaire, and any ETSS additional security requirements resulting therefrom are hereby incorporated by reference. The ETSS Security Questionnaire shall be supplied at the time of and as part of the proposal submission. The ETSS Security Questionnaire is also required for Vendors engaging in sole-source procurements, and as otherwise requested by the State.

(b) The Vendor's response to any ETSS Security Questionnaires shall be reviewed by the Chief Information Security Officer (CISO) (or the CISO's designee) and/or members of ETSS in accordance with established ETSS procedures.

(c) The Vendor is required to submit an ETSS Security Questionnaire with an applicable artifact if it demonstrates existing compliance with Service Organization Controls Reporting (SOC), Federal Risk and Authorization Management Program (FedRAMP), or State Risk Authorization Management Program (StateRAMP), or an equivalent (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable).

3. Multi-Factor Authentication ("MFA")

A. Definition

(i) MFA is an operational concept that requires more than one distinct authentication for successful authentication and/or access to an account.

B. Requirements for MFA

(i) Except as specifically provided in writing contained in a State solicitation document, all Vendors and their sub-processors who host, access, or manage data on State owned or managed environments or devices on behalf of the State are required to provide or support an MFA program for remote access in accordance with ETSS Policy 10-20, "Identification and Authentication for users, processes or devices," to enhance the security of such data. An ETSS designee shall review and determine whether the Vendor is MFA-compliant with the above.

(ii) "Non-public data" includes, but is not limited to, personally identifiable information (PII) and protected health information (PHI). PII is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." (NIST (SP) 800-53, under personally identifiable information from OMB Circular A-130 (2016) (Revision 5)). PHI is defined as information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer. (NIST SP 800-66 Rev. 1 from C.F.R., Sec. 160.103).

(iii) "Remote access" refers to any connection that enables users, devices, or systems to access the organization's information systems, services, or data from outside the organization's managed network environment. This includes, but is not limited to, access initiated over the public internet, through third-party networks, or from offsite locations such as home offices or mobile environments.

(iv) MFA must be enabled for all accounts and services that authenticate to systems that store, transmit, encrypt, or otherwise interact with State data including, but not limited to, those interactions where a login and/or password entry process is required.

C. Compliance and Auditing

(i) The State reserves the right to conduct a review and examination of relevant Vendor system records or compliance artifacts to test the adequacy and effectiveness of the overall security programs, data security, and data integrity procedures, to ensure compliance with the policies and operational procedures established herein, and to recommend any proposed changes. Any such access is subject to reasonable security requirements and excludes access to data or information of other Vendor clients and/or shared service infrastructure or environments. For purposes of this

Addendum and the Agreement, Vendor will comply with Vendor's security policies when using Vendor's systems and Vendor will comply with the State's security policies that are provided in advance when using the State's systems and ensure like protections or more robust within the Vendor's systems when hosting, storing, or processing State data as part of services provided.

D. Exceptions and Alternative Measures

(i) In circumstances where MFA cannot be feasibly implemented, Vendors and sub-processors within the service provided must seek written approval from the ETSS CISO for alternative security measures. Vendors shall submit detailed specifications of alternative security measures to the ETSS CISO. Any alternative measures must have a documented risk with an accompanying Plan of Actions and Milestones (POAM) and provide a level of security concerning the host, access, and/or management of data that is comparable to MFA. The ETSS CISO shall determine the level of security and, where appropriate, approve the use of alternative security measures with a documented risk acceptance. This determination shall be made at the time of proposal submission and required prior to proceed further with the solution proposed.

(ii) The State exclusively reserves the right to determine what MFA procedures shall be applicable.

4. <u>Artificial Intelligence ("AI") Requirements</u>

A. Definition

(i) AI is defined as a "machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action." (15 U.S.C. 9401(3)).

B. Restrictions on use of AI

(i) The Vendor agrees not to use any AI technologies provided by the State under this agreement for any purpose other than those expressly permitted in writing by the State. This includes a prohibition on modifying, reverse engineering, or creating derivative works from the AI technology, and using any related data or information for developing or enhancing AI models, without express written consent. Additionally, as agreed, the Vendor agrees to not employ the use of AI to influence otherwise permitted technologies like robotic process automation and machine learning.

C. Exceptions

(i) Due to the rapidly evolving nature of AI, the provisions of this section are subject to change, as applicable ETSS policies regarding the use of AI are implemented.

5. Accessibility and Useability Standard

(a) All web-based initiatives must follow the W3C Web Content Accessibility Guidelines 2.2, Level AA (WCAG 2.2 AA), the international standard of technical requirements to ensure digital public services are accessible to everyone. Vendor shall confirm that the service will meet (or exceed) WCAG 2.2 AA compliance by providing a Voluntary Product Accessibility Template (VPAT). If a VPAT is unavailable, a detailed description of service compatibility with commonly used assistive technologies must be included along with a description of the process used to test for accessibility compliance acceptable to the State.

6. Cybersecurity Requirements for Vendors

A. Access Control

(i) Unless otherwise provided, the Vendor and sub-processors within the service provided must confirm in writing their level of compliance with NIST (SP) 800-53, Section 3.1 "Access Control" (Revision 5). Vendor must conduct periodic reviews of its systems to ensure compliance with NIST (SP) 800-53, Section 3.1, "Access Control" (Revision 5). The Vendor must provide this confirmation with artifacts as needed at the time of proposal submission.

B. Awareness and Training

(i) The Vendor and sub-processors within the service provided must conduct security awareness and training programs for all personnel having access to the State of Rhode Island's data, emphasizing their roles and responsibilities in maintaining security. The Vendor shall conduct training in accordance with the standards set forth in NIST (SP) 800-53, Section 3.2, "Awareness and Training" (Revision 5). The Vendor must attest to having completed such training to the State. The State reserves the right to request a confirmation with artifacts from Vendor of the employees' completing Vendor's security awareness and training programs.

C. Audit and Accountability

(i) The Vendor is required to maintain internal logs of relevant system and user activities associated with the State of Rhode Island's data. These logs must be available for review upon request by the State of Rhode Island, and the Vendor must reasonably support and cooperate in any audit activities consistent with the parameters in 3(C)(i) above and applicable to sub-processors within the service provided.

D. Risk Assessment and Vulnerability Management

(i) The Vendor and sub-processors within the service provided must conduct periodic risk assessments of its information systems which handle and/or access the State of Rhode Island's data. Vulnerabilities must be addressed by severity in accordance with Enterprise Technology Strategy and Services guidance within 10-25 Risk Assessment Policy.

E. Incident Response

(i) The Vendor and sub-processors within the service provided must have an established incident response plan, including procedures for responding to security incidents and/data breaches that adhere to applicable local, state, and federal regulations. A data breach shall be understood to mean the loss of control, compromise, or unauthorized acquisition where: a person other than an authorized user accesses or is reasonably suspected to access data, such as personally identifiable information; or where an authorized user accesses non-public data, such as personally identifiable information, for an unauthorized purpose.

F. Physical and Environmental Protection

(i) The Vendor must ensure adequate physical security controls to protect data centers and computing resources from physical threats and environmental risks. Such controls must be in accordance with NIST (SP) 800-53, Section 3.11, "Physical and Environmental Protection" (Revision 5) and sub-processors within the service provided.

G. System and Communications Protection

(i) The Vendor and sub-processors within the service provided must implement measures to protect the integrity and confidentiality of data during transmission and rest. For encryption, State prefers a FIPS 140-2 or higher encryption mechanism at a minimum a 256-bit encryption mechanism shall be used.

(ii) Such measures must be in accordance with NIST (SP) 800-53, Section 3.18, "System and Communications Protection" (Revision 5).

H. System and Information Integrity

(i) The Vendor must ensure the integrity of its systems and data through measures like regular security patching, malware protection, and intrusion detection/prevention systems and sub-processors within the service provided. Such measures must be in accordance with NIST (SP) 800-53, Section 3.19, "System and Information Integrity" (Revision 5).

I. Compliance and Enforcement

(i) Failure to adhere to these requirements may result in termination of the contract, legal action, or other remedies as outlined in the terms and conditions agreed upon with the State of Rhode Island. Additionally, the State reserves the right to rescind the contract, according to the provisions governing termination, default, cancellation, and stop work found in the General Conditions of Purchase (220-RICR-30-00-13.20).

(ii) In circumstances where mitigation or resolution cannot be feasibly implemented, Vendors must seek written approval from the ETSS CISO for alternative security measures. Vendors shall submit detailed specifications of alternative security measures to the ETSS CISO. Any alternative measures must have a documented risk with an accompanying Plan of Actions and Milestones (POAM) and provide a level of security comparable to requirement deviating from. The ETSS CISO shall determine the level of security and, where appropriate, approve the use of alternative security measures with a documented risk acceptance. This determination shall be made at the time of proposal submission and required prior to proceed further with the solution proposed.

7. Data Breach Addendum to General Terms and Conditions

A. Responsibility in the Event of a Data Breach:

(i) All Vendors and sub-processors within the service provided are responsible for taking prompt action upon discovering or suspecting a data breach in accordance with the contract and/or Business Associate Agreement [BAA]. This includes breaches involving unauthorized access, disclosure, alteration, loss, or destruction of State of Rhode Island data. A data breach shall be understood to mean the loss of control, compromise, or unauthorized acquisition where: a person other than an authorized user accesses or is reasonably suspected to access non-public data, such as personally identifiable information; or where an authorized user accesses non-public data, such as personally identifiable information, for an unauthorized purpose.

(ii) Vendor and sub-processors within the service provided shall provide and pay for all remediation, services and costs associated with any data breach as agreed upon within the terms of the executed contract.

B. Reporting Data Breaches:

(i) Upon discovery, Vendors and sub-processors within the service provided must report any suspected or actual data breach to the CISO and the Chief Privacy Officer. All Vendors and subcontractors are responsible for being aware of and complying with the different notification time frames specifically required by

applicable laws, including, but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), relevant federal and state laws governing tax, the Rhode Island Identity Theft Protection Act, and other federal and state laws as applicable to Vendor as a service provider. Reports should include all relevant information about the breach, including the nature of the data involved, the specific circumstances of the breach, and any steps already taken in response.

C. Cooperation in Breach Investigation and Response:

(i) Upon reporting a breach, Vendors and sub-processors within the service provided are to reasonably cooperate with the State of Rhode Island's investigation and response efforts. This may include providing additional information, delivery of artifacts, allowing access to incident response retainer parties or service providers, refraining from certain activities, or participating in remediation actions.

D. Confidentiality During Breach Response:

(i) Vendors and sub-processors within the service provided must maintain the confidentiality of information related to the data breach investigation and response. Unauthorized disclosure of such information could impede the investigation and exacerbate the impact of the breach.

E. Liability and Consequences for Non-Compliance:

(i) Material failure to promptly report a data breach or reasonably cooperate in the breach response efforts may result in disciplinary action, up to and including termination of access, legal action, and or termination of the Agreement for cause.

F. Other Contract Provisions

(i) The provisions contained herein are in addition to any other contract provisions which may apply.