DATA SECURITY ADDENDUM

This Data Security Addendum ("**DSA**") sets forth Vendor's duties and obligations with respect to all Owner Data collected, used, transmitted or maintained for Owner, its instrumentalities, or its Affiliates. This DSA supplements the Agreement and in the event of any conflict between the terms of this DSA and the terms of the Agreement, the terms of this DSA will supersede and prevail. This DSA describes Owner's security requirements and sets forth Vendor's obligations to comply with such requirements.

1. DEFINITIONS

Definitions used in this DSA are available at [https://www.sanmanuel-nsn.gov/Procurement/Privacy-and-Data-Security] and are incorporated as if set forth herein.

2. DATA PRIVACY, ACCESS & USE

Vendor shall comply with the Data Processing Addendum ("**DPA**") available at [https://sanmanuel-nsn.gov/Procurement/Privacy-and-Data-Security], incorporated as if set forth herein.

3. INFORMATION SECURITY

a) **Security Program**. Vendor shall implement and maintain a written information security program (the "**Security Program**") applicable to all facilities, networks, infrastructure, devices, and cloud resources used by Vendor to provide the Services, including any applicable subcontractor facilities, networks, infrastructure, devices, and cloud resources. For purposes of this Agreement, Security Program shall include, but shall not be limited to, all Vendor policies, procedures, standards, and strategy, whether in hard copy, electronic, recorded form, or otherwise. The Security Program must contain reasonable and appropriate administrative, technical, and physical safeguards to monitor Vendor's systems and protect Owner Data against anticipated threats or hazards to its security, confidentiality, availability, or integrity; loss, or accidental, unlawful and unauthorized destruction, alteration, use, disclosure, acquisition, or access. Upon Owner's request, Vendor shall provide a written summary of the written information Security Program.

b) **Regular Testing, Assessing & Evaluation**. Vendor shall regularly, at least once every twelve (12) months and promptly after a Security Incident, assess risk, including risks to the privacy, security, integrity, and availability of Owner Data and test and monitor the effectiveness of its security safeguards, controls, countermeasures, systems and procedures including but not limited to: (i) vulnerability scanning; and (ii) penetration testing. Vendor will timely address any identified risks or effectiveness issues in its security safeguards, controls, countermeasures, systems and procedures.

c) **Safeguards**. At a minimum, Vendor's Security Program shall include:

i. Appropriate threat monitoring and detection pertaining to systems, databases, and/or infrastructure that store, transmit, or otherwise process Owner Data, including appropriate logging and anti-virus/anti-malware software;

ii. Vendor shall maintain, and provide to Owner upon request, audit logging a minimum of ninety (90) days or longer of user activity throughout the identity and access management lifecycle (e.g., session logon, logoff, lock, failed logon attempts, accurate date/time stamps, actions performed, non-repudiation, etc.).

iii. Security Incident response program;

iv. Use of secure user identification and authentication protocols, including, but not limited to, unique user credentials, use of appropriate access controls, and strict measures to protect identification and authentication processes. Vendor specifically acknowledges and agrees that it shall provide appropriate security to protect against unauthorized access by "insiders" (i.e., persons who have been given access to

Personal Data or systems containing Personal Data in order to perform computer related services for Customer, but who may intentionally or inadvertently cause damage to data or to the computer system). "**Insiders**" shall be deemed to include but shall not be limited to employees and former agents of Vendor, as applicable;

v. Patch-management program, whereby Vendor installs, within a commercially reasonable time following release taking into account the security severity rating, all security patches and operating system and application security updates for any devices or interfaces through which or with which the Services are provided;

vi. Use of encryption protocols at least at a level of HTTP with SSL 256-bit encryption (HTTPS) for Personal Data in transit and at rest, as appropriate and feasible;

vii. Implementation of secure coding practices pursuant to industry standards, such as those published by the Open Web Application Security Project;

viii. Secure remote access protocols and use of multi-factor authentication for access to computer systems;

ix. Appropriate network segmentation;

x. Password management, including requirements addressing complexity, storage and management, restrictions on password sharing, and account lockout controls;

xi. Training of appropriate personnel on all aspects of the items listed above.

d) **Security Incident**. Vendor shall notify Owner, within twenty-four (24) hours of discovery of the Security Incident. To the extent known, such notification shall include: (a) the nature of the Security Incident; (b) the date and time the Security Incident occurred including when it was discovered; (c) the number of Individuals affected by the Security Incident; (d) the categories of Personal Data involved; (e) the measures that were taken to address the Security Incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the Security Incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the Security Incident. Vendor shall take all appropriate corrective action, at Vendor's sole cost and expense, to prevent a recurrence of such Security Incident.

e) **Cooperation**. Vendor shall provide Owner with all such timely information and cooperation as Owner may require to fulfill its data breach reporting obligations under (and in accordance with applicable regulatory timelines) Data Protection Laws. Unless required by Data Protection Laws, Owner alone may notify any Regulator. Vendor shall refrain from making public announcements regarding such Security Incident without Owner's prior written approval. Upon Owner's request and pursuant to Owner's instructions, Vendor shall assist with or perform all remediation efforts required by Data Protection Laws. Vendor shall not issue any press release or public statement regarding a Security Incident without the prior written consent of Owner. For the avoidance of doubt, to the extent the Security Incident relates to or results from Vendor's action or inaction, Vendor shall be solely responsible for the costs and expenses of all remediation measures.

f) **Business Continuity & Recovery**. Vendor shall maintain a business continuity program, including a recovery plan, designed to ensure Vendor can continue to function and provide Service to Owner through an operational interruption. The program shall provide a framework and methodology, including a business impact analysis and risk assessment process, necessary to identify and prioritize critical business functions. If Vendor experiences an event requiring recovery of systems, information or services, the recovery plan will be executed promptly. Vendor shall continuously enhance the security and availability of its infrastructure. Vendor shall ensure that Vendor's business continuity and recovery program provides for any period of unavailability of Vendor systems and Services to Owner after a ransomware attack, failure or disaster to be no longer than 48hours. Vendor shall maintain immutable backups to ensure that Vendor can restore Vendor systems and Services such that, upon a recovery from a ransomware attack, failure or disaster, the Owner Data will be restored to a point no more than 24 hours before the failure or disaster. Vendor shall ensure that processing can be properly resumed in the event of failures, which include mechanical, electronic or communication failure. Vendor shall test its business continuity and recovery plan at least once annually and provide results to Owner if requested. The Vendor shall also provide Owner with a copy of updated versions of the business continuity and recovery plan of Vendor (and any third-party hosting company that it uses) within five (5) days of Owner requesting a copy. Owner shall be free to share the disaster plan with any government agency with jurisdiction to request a copy from Owner.

g) **Key Management**. Vendor shall use encryption keys all around the hosted software applications that are used to provide the Service, including but not limited to secure storage, secure transport, token generation, and authentication. Vendor shall ensure the hosted software application used to provide the Service does not utilize a single centralized key-store for both architecture and security reasons. Vendor shall ensure the different keys are stored by different means in accordance with their availability and security requirements.

h) **Open Source**. Any open-source code used in Vendor's Services must be inventoried and evaluated for security vulnerability. Vendor will document all third-party software used in the Services (i.e., libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source), and Vendor will make the document available to Owner when security investigation is required.

i) **Security Questionnaires**. No more frequently than once per twelve (12) month period, upon written request by Owner, Vendor shall respond to security questionnaires provided by Owner with regard to the Security Program, provided that disclosure of any such information will not compromise Vendor's confidentiality obligations and/or legal obligations or privileges.

j) **Audit**. Owner reserves the right to request evidence of Vendor's third-party audits (e.g., Service Organization Control (SOC) 2), at Owner's discretion. If applicable, Owner, and any governmental entity with jurisdiction or oversight authority, may, upon prior notice to Vendor, audit Vendor's records of Owner's Confidential Information and speak with Vendor's personnel who are familiar with such records. Such audits shall include, but not be limited to, auditing for compliance with this DSA and Owner (and its designated auditor) shall be entitled to receive audit reports by qualified auditing entities confirming Vendor's compliance with standards relating to bias, accountability, compliance with law, and revisions and updates to any artificial intelligence systems. Owner shall have the right to provide copies of any such audit to its applicable regulator(s).

4. MISCELLANEOUS

a) **Termination**. This DSA shall end automatically when the Agreement is terminated or expires. In the case of any non-compliance by Vendor Parties with any of the obligations under this DSA, the Data Protection Laws, and/or Owner's instructions, Owner may, by giving written notice, immediately terminate the Agreement and/or suspend any data submission under the Agreement and/or require Vendor to cease or suspend any Processing or use of Owner Data.

b) **Obligations Post-Termination**. Termination or expiration of the DSA shall not discharge Vendor from its obligations meant to survive the termination or expiration of the DSA.

c) **Severability**. Any provision of the DSA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this Agreement.

d) **Modifications and Amendments**. The DSA may only be amended by a written instrument executed by the parties.