DASNY's Security Requirement

Purpose:

This document sets forth the information security program and infrastructure policies that an organization shall meet and maintain in order to protect DASNY Data from unauthorized use, access, or disclosure. Such program and policies shall satisfy DASNY's requirements applicable to the Vendor System under the Agreement. The following summarizes requirements from DASNY Policies, New York State (NYS) Information Technology Services (ITS) Policies and other applicable governmental authorities. Any future applicable changes to NYS ITS, or a governmental authority's, policies during the term of an agreement shall be incorporated into these security requirements.

Information Security Management Program:

Any organization shall represent, warrant and covenant that it shall maintain throughout the Term of an Agreement a written information security management program ("**ISMP**") designed to protect and secure DASNY Data from unauthorized access, use or disclosure. The ISMP will be documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices and industry standards.

Certifications:

During the Term of any Agreement, an organization will implement and maintain administrative, physical, and technical safeguards and measures designed to: (a) ensure the security and integrity of DASNY Data, and (b) protect against unauthorized access to DASNY Data and DASNY's IT systems. Such security program will conform to the Security Services requirements and an organization's most recently completed SSAE18 or SOC2 Type II audit report (or industry-standard substantially similar reports) (collectively referred to as "**Audit Reports**") to the extent satisfactory to DASNY. The organization shall provide these to DASNY on the anniversary of the Effective Date during the Term and at other times as DASNY requires for meeting requirements imposed on or requests made to it. In no event during the Term will an organization materially diminish the protections provided by the controls set forth. An organization represents that the specifications and requirements set forth satisfy DASNY's security requirements disclosed to any organization.

Access Controls:

An organization will restrict access by its Representatives to DASNY data using the principal of least privilege and will take all reasonable steps to prevent anyone from accessing DASNY data in any manner or for any purpose not authorized by DASNY and the Agreement. An organization shall limit access to DASNY data to any organization's Third Parties who (1) have a legitimate need to access DASNY data to provide services pursuant to the Agreement, and (2) have agreed in writing to protect the integrity, availability and confidentiality of DASNY data.

No later than the anniversary date of the Effective Date in each year of the Term, an organization's senior executive skilled in security will meet the DASNY Representative(s) designated by the

DASNY to discuss in good faith the adoption of new technology and improvements in practices to provide increased security and data protection. The Parties recognize that cyber threats have become more sophisticated, and it is both Parties' intention to enhance the security measures provided.

DASNY (and any governmental authority having jurisdiction over the DASNY) shall have the right to conduct audits of an organization's compliance with the security requirements in a manner that is designed to minimize disruption to an organization's normal business operations. The right to audit includes the right to audit access logs and other logs recording the identity of parties having access to the DASNY Data.

Review Process:

Upon request the Vendor must cooperate with DASNY on a security assessment. An organization is obligated to certify compliance with the following:

- Complete security questionnaires as requested by DASNY's Chief Information Security Officer.
- Provide a copy, abstract or otherwise make available for review all required supporting documents that align with the services and support provided as requested by DASNY's Chief Information Security Officer.
- Allow verification of environmental and physical security controls at IT and business facilities where DASNY data is stored and where a current SSAE18 or equivalent comparable assessment acceptable to DASNY was conducted and a copy of the report provided to DASNY.
- Provide a commitment in writing, with target dates, to address issues identified in applicable DASNY assessment reports.

Security Policy:

An organization will maintain a comprehensive information security policy that governs the personal data used in the services being provided to DASNY and the security policy must be reviewed and/or updated by the organization at least annually.

Security Training:

Each Vendor Representative with access to DASNY Data shall receive annual training on the organization's ISMP and demonstrate his/her ability to comply with the Security Services requirements applicable to such Representative's services.

Application Security:

An organization will install a then-current leading edge, enterprise application to prevent the introduction of Harmful Code. The organization agrees at all times to provide, maintain and support its Software and subsequent updates, upgrades, and bug fixes such that the Software is, and remains secure from those vulnerabilities.

An organization will ensure that application software provided to DASNY is part of recurring, annual web application vulnerability scans conducted by an independent third party to identify and correct all security vulnerabilities within the application in a timeframe commensurate with industry best practices. Upon request the organization will provide DASNY with an abstract from a recent web application vulnerability scan conducted by an independent third party. The organization must remediate all issues identified by DASNY in a timeframe commensurate with industry best practices.

An organization will ensure that application software supports Multi Factor Authentication (MFA) for all user access. SMS based One Time Passcodes (OTPs) cannot be used as a primary, or secondary, factor. Email OTPs must be configured to only be sent to approved DASNY email accounts. The software shall at a minimum support 3 factors for authentication.

An organization must ensure that software has the capability of meeting the minimum following password complexity rules.

- Be at least 12 positions in length.
- Contain a mix of alphabetic and non-alphabetic characters (numbers, punctuation or special characters) or a mix of at least two types of non-alphabetic characters.
- Not contain the userid as part of the password.
- Be changed at least once every year or upon indications of compromise.
- Not be reused for at least 2 years or utilized within the last 12 prior password leveraged by the user.
- Maximum of 5 unsuccessful logon attempts before lockout.
- Be set to an expired state when issued or reset unless system generated.

Data Security:

Uploading and downloading of DASNY Data and User Data must be performed through an encrypted and secure connection by using Hypertext Transfer Protocol Security ("HTTPS"). Encryption for data in transit shall include, but not be limited to, Transport Layer Security ("TLS") 1.3 or later and maintaining at all times a secure protocol based on industry best practices. An organization will maintain 24/7 monitoring sufficient to enable it to respond to and limit the effects of security incidents, intrusion attempts and/or weakness in the organization's IT Infrastructure.

Encryption:

If DASNY shares information with an organization (e.g., system logs or data files) the organization must encrypt the following: (a) Non-public DASNY data in storage / at rest, (b) Laptops, (c) Backup tapes / media, (d) Removable Media (e.g. CDs, USB drives, thumb drives) must either be encrypted or disabled from use.

Note, all references to encryption must meet, at the time of encryption, current NIST minimum bit length.