APPENDIX C-1

ITS-AGS: INFORMATION SECURITY STANDARDS

Table of Contents

1. Secure System Development Life Cycle Standard

ITS has defined a Secure Systems Development Lifecycle (SSDLC) based on the NIST framework. These SSDLC security requirements and tasks must be considered and addressed within every system, project or application and sufficiently documented to demonstrate the extent to which each security activity is applied.

At a minimum, a SSDLC must contain the following security activities:

1. Define Security Roles and Responsibilities
2. Orient Staff to the SDLC Security Tasks
3. Establish a System Criticality Level
4. Classify Information
5. Establish System Identity Assurance Level Requirements
6. Establish System Security Profile Objectives
7. Create a System Profile
8. Decompose the System
9. Assess Vulnerabilities and Threats
10. Assess Risks
11. Select and Document Security Controls
12. Create Test Data
13. Test Security Controls
14. Perform Certification and Accreditation
15. Manage and Control Change
16. Measure Security Compliance
17. Perform System Disposal

Additional information is found in policy *NYS-S13-001 Secure System Development Life Cycle*, see Table 1 in section 2.

2. New York State Information Technology Security Policies

Every system, project or application must comply with the New York State Information Technology Security Policies, published by the NYS Enterprise Information Security Office (EISO) at its.ny.gov/eiso/policies/security, that are applicable to it. These policies are listed in the table below.

Table 1

NYS-P03-002	Information Security Policy
NYS-P10-006	Identity Assurance Policy

NYS-P13-001	Information Security Exception Policy
NYS-P14-001	Acceptable Use of Information Technology (IT) Resources Policy
NYS-S10-001	CPE Requirements for ISOs/Designated Security Representatives Standard
NYS-S13-001	Secure System Development Life Cycle (SSDLC) Standard
NYS-S13-002	Secure Coding Standard
NYS-S13-003	Sanitization/Secure Disposal Standard
NYS-S13-004	Identity Assurance Standard
NYS-S13-005	Cyber Incident Response Standard
NYS-S14-001	Information Security Risk Management Standard
NYS-S14-002	Information Classification Standard
NYS-S14-003	Information Security Controls Standard
NYS-S14-005	Security Logging Standard
NYS-S14-006	Authentication Tokens Standard
NYS-S14-007	Encryption Standard
NYS-S14-008	Secure Configuration Standard
NYS-S14-009	Mobile Device Security Standard
NYS-S14-010	Remote Access Standard
NYS-S14-013	Account Management / Access Control Standard
NYS-S15-001	Patch Management Standard
NYS-S15-002	Vulnerability Scanning Standard
NYS-S15-003	Wireless Technology Standard
NYS-G10-001	Secure Use of Social Media Guideline

3. Information Security and Emergency Procedures

New York State considers the security and protection of State information to be a critical aspect of this engagement.

Contractor agrees to comply with the following requirements:

- Comply with all federal and state security policies in relation to providing services to ensure the confidentiality, integrity and availability (CIA) of NYS data.

- NYS follows NIST 800-53 guidelines for implementing system security and privacy controls. Vendors should also be aware of the FedRAMP program when implementing systems for NYS.

- Run NYS Enterprise Information Security Office (EISO) approved security scans specified in policy *NYS-S15-002 Vulnerability Scanning Standard* prior to the launch of any major changes to the [enter project name], as well as follow policy *NYS-S13-001 Secure System Development Life Cycle*.

- Undergo a data classification in conjunction with [enter agency name] to identify the criticality of the data being collected and stored.

- Share all vendor's third party audit reports with the State.

- Allow the State to verify implementation of recommendations resulting from the third party audits.

- In the event of a security breach, as defined by State Technology law Section 208, the Contractor shall act in accordance with New York State Breach Notification Law.

- Contractor is required to submit, as part of its overall security plan, a Protection and Risk Assessment Plan for the management of the State's confidential information. The Protection and Risk Assessment Plan is expected to include Contractor's technology- and non-technology-based process for securing the State's confidential information. At a minimum, the Protection and Risk Assessment Plan must address the areas listed below.

  - Ensuring and certifying that employees, subcontractors, and business partners are aware of and comply with NYS information security and confidentiality requirements.

  - Documentation to detail the extent to which each security activity listed in section *1. Secure System Development Life Cycle Standard* is followed.

  - Security reviews and audits, including third-party reviews, audits, and facility audits.

  - Use of security tools and standards (e.g., security software, encryption standards, etc.).

  - Maintaining and enhancing the bidder’s information security environment and business practices with procedures and policies for a security environment aligning with industry best practices.

Contractor is expected to provide copies of Continuance of Operations Plan (COOP) and Disaster Recovery Plan (DRP) plans for all data, records, forms, and data processing operations associated with [enter project name]. **The following areas should be addressed as part of the security documentation:**

- Establish procedures to ensure its data processing system will be back in at least minimal operation within [insert time constraint].

- Ensure complete, accurate and up-to-date documentation of all systems and procedures used to operate [enter project name]. This documentation shall include a back-up copy stored encrypted, where appropriate, off premises (New York State data should not reside outside of the continental United States).

- Redundant architectures, based on the criticality of data, e.g. Tier III data center; regular file back-ups; and continuous 24-hour monitoring required for hosted environments.

- Provide recovery procedure training for all personnel and refresher training at least annually.

4. Cloud Security Requirements

If cloud based services are a component of the solution or services to be provided by Contractor, Contractor must comply with FedRAMP (https://www.fedramp.gov) standards for cloud services, and other applicable federal and New York State laws, regulations and requirements.