APPENDIX C

ITS-DCS: INFORMATION SECURITY STANDARDS

Table of Contents

1. Secure System Development Life Cycle Standard

ITS-DCS 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*, https://its.ny.gov/document/secure-system-development-life-cycle-ssdlc-standard.

2. New York State Information Technology Security Policies

Every system, project or application must comply with the New York State Information Technology Security Policies, Standards and Procedures published by the NYS Enterprise Information Security Office (EISO) at its.ny.gov/eiso/policies/security, that are applicable to the services being provided by Contractor.

All expenses, including travel and lodging associated with compliance of the Contractor Staff to these security requirements are the responsibility of the Contractor and are not reimbursable. In addition, Contractor shall comply fully with all other security policies, standards and procedures, not identified in this solicitation, of the State clearly communicated to it in the performance of this project, as long as compliance with such procedures does not result in a substantial or material increase in cost to Contractor.

Contractor further warrants that its staff (employees, agents and subcontractors) are properly informed regarding security standards and are prohibited from disclosing confidential information to any persons without a need to know.

If any software application or vulnerability security scanning undertaken reveals vulnerabilities or any other security risks attendant to the provided solution Contractor is responsible for ensuring those vulnerabilities and risks are promptly remediated to DCS's reasonable satisfaction.

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 laws, regulations and policies in relation to providing services to ensure the confidentiality, integrity and availability (CIA) of NYS data.

- Security for the State's data hosted by Contractor or its subcontractors, if any, is the responsibility of Contractor and will not require customization by DCS.

- 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 Employee Benefit Card Project Services, as well as follow policy *NYS-S13-001 Secure System Development Life Cycle*.

- Share all vendor’s third party audit reports with the State within 60 days of completion.

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

- 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. of the 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 Employee Benefit Card Project Services. **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 four (4) hours of loss of Project services.

- Ensure complete, accurate and up-to-date documentation of all systems and procedures used to operate the Employee Benefit Card Project Services. 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.