System and Services Acquisition Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Reviewed Date – 03/29/2024

1. Purpose

Ensure the establishment of security measures that address the risk that may arise from the acquisition of systems and services utilized by the District of Columbia Government (District).

2. Authority

DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer (OCTO) with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District. This document can be found at: *https://code.dccouncil.us/dc/council/code/sections/1-1402*.

3. Applicability

This policy applies to all District workforce members (including contractors, vendors, consultants, temporary staff, interns, and volunteers) performing official functions on behalf of the District, and/or any District agency or entity (e.g. subordinate and independent agencies, Council of the District of Columbia, D.C. Charter Schools, etc.) who receive enterprise services from OCTO. In addition, this policy applies to any provider or third-party entity with access to District information, networks, and applications.

4. Policy

District agencies and departments must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Allocation of Resources

The District agency must:

4.1.1. Determine information security requirements for the information system or information system service in mission/business process planning.

4.1.2. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.

4.1.3. Establish a discrete line item for information security in organizational programming and budgeting documentation.

4.2. System Development Life Cycle

The District agency must:

4.2.1. Manage the information system using the District System Development Lifecycle and the District Software Development Lifecycle that incorporates information security considerations.

4.2.2. Define and document information security roles and responsibilities throughout the system development life cycle.

4.2.3. Identify individuals having information security roles and responsibilities.

4.2.4. Integrate the organizational information security risk management process into system development life cycle activities.

4.3. Acquisition Process

The District agency must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service per applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

4.3.1. Security functional requirements.

4.3.2. Security strength requirements.

4.3.3. Security assurance requirements.

4.3.4. Security-related documentation requirements.

4.3.5. Requirements for protecting security-related documentation.

4.3.6. Description of the information system development environment and the environment in which the system is intended to operate.

4.3.7. Acceptance criteria.

4.4. Information System Documentation

The District agency must:

4.4.1. Obtain administrator documentation for the information system, system component, or information system service that describes:

- Secure configuration, installation, and operation of the system, component, or service
- Effective use and maintenance of security functions/mechanisms
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions

4.4.2. Obtain user documentation for the information system, system component, or information system service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms
- Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner
- User responsibilities in maintaining the security of the system, component, or service

4.4.3. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes appropriate action in terms of penalties as documented in the contract in response.

4.4.4. Protect documentation as required, per the risk management strategy.

4.4.5. Distribute documentation to relevant stakeholders that need to know.

4.5. Security and Privacy Engineering Principles

The District agency must apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of the information system.

4.6. External Information System Services

The District agency must:

4.6.1. Require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.6.2. Define and documents government oversight and user roles and responsibilities regarding external information system services.

4.6.3. Employ checks to monitor security control compliance by external service providers on an ongoing basis.

4.7. Developer Configuration Management

The District agency must require the developer of the information system, system component, or information system service to:

4.7.1. Perform configuration management throughout system, component, or service design during all phases of the Software Development Lifecycle (SDLC).

4.7.2. Document, manage, and control the integrity of changes to the defined configuration items that are under configuration management.

4.7.3. Implement only approved changes to the system, component, or service.

4.7.4. Document approved changes to the system, component, or service and the potential security impacts of such changes.

4.7.5. Track security flaws and flaw resolution within the system, component, or service and report findings.

4.8. Developer Testing and Evaluation

The District agency must require the developer of the information system, system component, or information system service to:

4.8.1. Create and implement a security assessment plan.

4.8.2. Perform unit; integration; system; regression testing/evaluation.

4.8.3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.

4.8.4. Implement a verifiable flaw remediation process.

4.8.5. Correct flaws identified during security testing/evaluation.

4.9. Unsupported System Components

The District agency must replace systems and/or components when support for the components is no longer available from the developer, vendor, or manufacturer.

5. Exemptions

Exceptions to this policy shall be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO) for approval.

6. Definitions

The definition of the terms used in this document can be found on the *Policy Definitions website*.