Information Security Program Management Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Reviewed Date – 05/17/2024

1. Purpose

Effective program management ensures that security considerations are planned for early and handled consistently throughout its lifecycle. The Government of the District of Columbia (District) has established an integrated enterprise-wide decision structure for cybersecurity risk management that includes cybersecurity requirements for the District's information technologies.

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.gov/us/dc/council/code/sections/1-1402.

3. Applicability

This policy applies to all District workforce members responsible for application identity and role definition on behalf of the District, and/or any District agency/District/entity who receive enterprise services from OCTO. In addition, this policy applies to any provider and third-party entity with access to District information, systems, networks, and applications.

4. Policy

District agencies that fall under the authority of the Mayor of the District, must protect and control electronic and physical data while at rest and in transit. The District agency will take appropriate safeguards for protecting the District's data to limit potential mishandling or loss while being stored, accessed, or transported. The District must assess any inadvertent or inappropriate data disclosure and/or use must be reported to the concerned Agency's Senior Information Security Officer (SISO), the SOC, and CISO. All the District agencies must develop or adopt OCTO's procedures that must define requirements for the secure handling, transporting, and storing media. The following requirements must be defined in the procedure. 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. OCTO will review, update, and disseminate this policy annually at a minimum, to ensure accuracy, clarity, and completeness. 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. Information Security Program Plan

The District agency must:

4.1.1. Develop and disseminate an organization-wide information security program plan that:

- Provides an overview of the information security program requirements, a description of the information security program management controls, and the administrative, technical, and physical controls in place or planned for meeting those requirements
- Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical)
- Ensures that the program is approved by the District Agency's Director with a clear definition of roles, responsibility, and accountability for the risk being incurred to the agency's operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation

4.1.2. Ensures the plan is reviewed annually and updated when organizational changes occur.

4.1.3. Ensures updates to the plan address problems identified during plan implementation or security control assessments.

4.1.4. Protects the information security program plan from unauthorized disclosure and modification.

4.2. Senior Information Security Officer

The District agency must appoint a Senior Information Security Officer (SISO) with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

4.3. Information Security Resources

The District agency must:

4.3.1. Ensure that capital planning and investment requests include the resources needed to implement the information security program and document all exceptions to this requirement.

4.3.2. Employ a business case to record the resources required.

4.3.3. Ensure that information security resources are available for expenditure.

4.4. Plan of Action and Milestones (POA&M) Process

The District agency must:

4.4.1. Implement a process to ensure that plans of action and milestones for the information security program and associated organizational information systems:

- Are developed and maintained
- Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation
- Are reported per OMB FISMA reporting requirements

4.4.2. Review plans of action and milestones for consistency with City-wide risk posture goals as well as organizational risk management strategy and organization-wide priorities for risk response actions.

4.5. Information System Inventory

The District agency must develop and maintain an inventory of their information systems.

4.6. Information Security Measures of Performance

The District agency must develop, monitor, and report on the results of information security measures of performance.

4.7. Enterprise Architecture

The District agency must develop and maintain an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

4.8. Critical Infrastructure Plan

The District agency must address information security issues in the development, documentation, and updating of critical infrastructure and key resources protection plans.

4.9. Risk Management Strategy

District agencies must:

4.9.1. Develop a comprehensive strategy to manage IT risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.

4.9.2. Implement the risk management strategy consistently across the organization.

4.9.3. Review and update the risk management strategy annually or as required to address organizational changes.

4.9.4. Submit to the CWITS-required Risk Management Process, in accordance with the Risk Assessment Policy

4.10. Security Authorization Process

District agencies must:

4.10.1. Manage (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through internal and CWITS-required security authorization processes.

4.10.2. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process.

4.10.3. Fully integrate the security authorization processes into an organization-wide risk management program.

4.11. Mission/Business Process Definition

District agency must:

4.11.1. Define mission and business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

4.11.2. Determine information protection needs arising from the defined mission and business processes.

4.11.3. Review and revise the mission and business processes as necessary, until achievable protection needs are met.

4.12. Insider Threat Program

The District agency must implement an insider threat program that includes a cross-discipline insider threat incident handling team.

4.13. Information Security Workforce

The District agency must establish an information security workforce development and improvement program.

4.14. Testing, Training, and Monitoring Security Workforce

The District agency must:

4.14.1. Implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

- Are developed and maintained
- Continue to be executed promptly

4.14.2. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy.

4.15. Contacts with Security Groups and Associations

The District agency must establish and institutionalize contact with selected groups and associations within the security communities to:

4.15.1. Facilitate ongoing security education and training for organizational personnel.

4.15.2. Maintain currency with recommended security practices, techniques, and technologies.

4.15.3. Share current security-related information including threats, vulnerabilities, and incidents.

4.16. Threat Awareness Program

The District agency must implement a threat awareness program that includes a cross-organization information-sharing capability for increased threat awareness.

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 in the *Policy Definitions* website.