Compliance Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Review Date – 03/01/2024

1. Purpose

Establish a consistent and effective framework for monitoring, measurement, and analysis of compliance with information security policies, standards, and procedures, as well as the performance and the effectiveness of the Cyber Security Framework (CSF). Furthermore, this policy concerns itself with avoidance of legal, statutory, regulatory, or contractual obligation breaches related to information security.

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 of Columbia Government (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. Monitoring, measurement, analysis, and evaluation

All District agencies must evaluate the information security performance and the effectiveness of information security controls.

All District agencies must determine:

4.1.1. What needs to be monitored and measured, including information security processes and controls.
4.1.2. The methods for monitoring, measurement, analysis, and evaluation, as applicable, ensure valid results.
4.1.3. When the monitoring and measuring must be performed.
4.1.4. The employee is responsible for conducting the monitoring and measurement

for compliance.

4.1.5. When the results from monitoring and measurement must be analyzed and evaluated.

4.1.6. The employee responsible for analyzing and evaluating the results from monitoring and measurement.

All District agencies must retain appropriate documented information as evidence of the monitoring and measurement results.

4.2. Internal audit/Independent Reviews

4.2.1. All District agencies must conduct internal audits annually at a minimum or when significant changes occur, to provide information on whether the information security controls conform to requirements stipulated by published IT Security Policies, regulatory requirements, legal obligations through existing contracts, and NIST SP 800-53.

4.2.2. The independent reviews must include testing of controls, policies, processes, and procedures for information security and document the results of the testing.

4.3. Information systems audit controls

Audit requirements and activities involving verification of operational systems must be carefully planned and agreed to minimize disruptions to business processes.

4.4. Management review

The District CISO will review all District Policies annually to ensure its continuing suitability, adequacy, and effectiveness. The review must include consideration of:

The status of actions from previous reviews.

4.4.1. Changes in external and internal issues that are relevant to the security policies.

4.4.2. Feedback on the information security performance, including trends in nonconformities and corrective actions, monitoring and measurement results, audit results, and fulfillment of information security objectives.

4.4.3. Feedback from interested parties.

4.4.4. Results of risk assessment and status of the risk treatment plan.

4.4.5. Opportunities for continual improvement.

The outputs of the CISO review must include decisions related to continual improvement opportunities and any needs for changes to the District Information Security Program. The CISO must retain documented information as evidence of the results of reviews.

4.5. Compliance with security policies and standards

System Managers must regularly review the compliance of information processing and procedures (SOPs) within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

4.6. Technical compliance review

Information systems must be regularly reviewed for compliance with the District information security policies and standards.

4.7. Noncompliance and corrective action

Corrective actions must be appropriate to the effects of the nonconformities encountered. When noncompliance occurs, District agencies must:

4.7.1. React to the noncompliance and as applicable take action to control and correct it and deal with the consequences.

4.7.2. Evaluate the need for action to eliminate the causes of non-compliance, so that it does not recur or occur elsewhere, by:

- Reviewing the noncompliance
- Determining the causes of the noncompliance
- Determining if similar non-compliance exist or could potentially occur
- Implementing any action needed
- Reviewing the effectiveness of any corrective action taken
- Making changes to the information security management system, if necessary

4.7.3. District agencies must retain documented information as evidence of:

- The nature of the noncompliance and any subsequent actions taken
- The results of any corrective action taken

4.8. Continuous Improvement

All District agencies must continually improve the suitability, adequacy, and effectiveness of their information systems.

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.