Configuration Management Policy

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

1. Purpose

Ensure that all configuration changes to the District of Columbia Government (District) owned information assets and resources are conducted with appropriate oversight, knowledge, and consent, is appropriately tested, and does not introduce security weaknesses to the District's overall IT security risk posture.

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 government. 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 (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. 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 change to the policy, a procedure in support of this policy with the following requirements.

4.1. Baseline Configuration

District agencies must provide common security configurations that provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This requirement will allow the District agencies to improve information system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of District data.

4.2. Security Impact Analysis

All District agencies must analyze changes to the information system to determine potential security impacts prior to change. System Owners will conduct a security impact analysis to determine which controls will be assessed for proper implementation and operation.

Security impact analysis may include, for example, reviewing system plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls.

4.3. Access Restrictions For Change

All District agencies must define, document, approve and enforce physical and logical access restrictions associated with changes to the information system. Only qualified and authorized District workforce members can be granted access to the system to initiate changes, including upgrades and modifications.

4.4. Configuration Settings

All District agencies must:

4.4.1. Establish and document configuration settings for information technology applications and technologies deployed within their information system in accordance with Center for Internet Security (CIS) benchmarks for servers and network devices as part of configuration files that reflect the most restrictive mode consistent with operational requirements.

4.4.2. Implement the configuration settings.

4.4.3. Identify, document, and approve any deviations from established configuration settings for information systems based on CIS benchmarking of information systems.

4.4.4. Monitor and control changes to the configuration settings in accordance with District agency policies and procedures.

4.5. Least Functionality

All District agencies must configure information systems to provide only essential capabilities and prohibit the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.

4.6. Information System Component Inventory

All District agencies must:

4.6.1. Develop and document an inventory of information system components that:

- Accurately reflects the current information system
- Includes all components within the authorization boundary
- Is at the level of granularity deemed necessary and appropriate for tracking and reporting
- Includes an information system component inventory for servers, workstations, network devices, and peripheral devices maintained and monitored through the enterprise hardware/software asset management tool

4.6.2. Reviews and updates the information system component inventory annually and as required.

4.7. Software Usage Restrictions

All District agencies are required to:

4.7.1. Use software and associated documentation in accordance with contract agreements and copyright laws.

4.7.2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

4.7.3. Control and document the use of peer-to-peer file-sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

4.8. User Installed Software

All District agencies must:

4.8.1. Establish the policies governing the installation of software by users.

4.8.2. Enforce software installation policies through the IT asset management process.

4.8.3. Monitor user compliance with this policy on a continual basis.

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*.