Asset Management Policy

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

1. Purpose

Establish an effective and consistent approach for appropriately protecting the confidentiality, integrity, and availability of information assets per their importance to the Government of the District of Columbia (District) by laying down requirements for the ownership, categorization, acceptable use, and secure handling of information assets.

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. Asset Acquisition

The acquisition of information assets for the District must be obtained per the System and Services Acquisition Policy.

4.2. Asset Management

All District agencies shall allocate asset management responsibilities to designated resources responsible for the identification, verification, and recording of every information asset owned by the respective agency.

4.3. Asset Identification

Every information asset must have a tag that contains the identification information relevant to such an asset.

4.4. Inventory of Assets

Assets owned and associated with the District information and information processing facilities must be identified, and an inventory of these assets shall be created and maintained.

4.5. Asset Security

Assets listed in the inventory must have their security regularly reviewed and maintained by an agency-level Information Security Team or by the District Information Security Team. The security of the assets must include how such assets and information are secured while used remotely.

4.6. Security Categorization

All District information assets must be categorized based on the assessment of the potential impact that a loss of confidentiality, integrity, or availability of such asset, and the information contained in it, would have on the District operations, workforce, clients, and partners.

4.7. Acceptable Use of Assets

The use of the information assets must be in accordance with the District's *Acceptable Use Policy (AUP)*. The AUP stipulates the rules for the acceptable use of the District information, and the assets associated with such information.

4.8. Asset Issuance

Before a District-owned asset is issued to any District workforce member, an agency-level asset inventory record must be updated to reflect the current holder/owner of the asset. In addition, as assets are refreshed or rotate possession, that asset inventory record must be updated to reflect the status.

4.9. Return of Asset

All District workforce members must return issued assets in their possession upon their separation from the District.

4.10. Disposal of Asset

Every District-owned asset that has been retired and approved for disposal must be erased securely in a way that ensures that all District sensitive data is made irrevocable during or before the asset's disposal.

5. Exemption

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*.