Information System Change Control Policy

Approved Date – 02/22/2016
Published Date – 02/22/2016
Review Date – 05/17/2024

1. Purpose

Provide the requirement for agencies to implement an information system change control process to protect the confidentiality, integrity, and availability of information systems.

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.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 who receive enterprise services from OCTO. This Policy also applies to any providers and third-party entities 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 change to the policy, a procedure in support of this policy with the following requirements:

4.1. Change Advisory Board
Each Agency Chief Information Officer (CIO) shall consult with the OCTO Change Advisory Board (CAB) in which each agency plans and coordinates all system changes within the District enterprise with the OCTO CAB. The CAB must evaluate all information system and security configuration changes before implementation. The OCTO CAB must approve, disapprove, or modify a system change.

4.2. Change Manager
The OCTO Change Manager is the member of the CAB who ensures the change request is following the standardized operating procedure. The OCTO Change Manager can authorize the change. In addition, the OCTO Change Manager ensures timely decision-making for change requests.

4.3. Change Owner/Initiator

Each Agency ClO must designate a Change Owner or Initiator who must act as the liaison with the OCTO CAB, to track all agency system change requests, and report all CAB-approved system changes to the DC Chief Technology Officer through the CAB. The Change Owner/Initiator must be a District Government employee.

4.4. CAB Membership

Representatives from each OCTO department and the Change Manager are the members of the CAB. Each Agency CIO must ensure that the CAB meeting is joined by the IT technical and security personnel, as well as management officials who understand the impacts of the proposed information system changes to provide relevant and knowledgeable advice to the OCTO Change Manager.

4.5. Security Impact Analysis

Each agency must ensure that each proposed information system change, or security configuration is analyzed for potential impacts on the confidentiality, integrity, and availability of the information system and the data contained therein before change approval and implementation.

4.6. Pre-Change Validation

Each Agency Change Owner/Initiator must ensure that each proposed information system or security configuration change is documented, tested, and validated before change approval and implementation.

4.7. System Access for Change Implementers

Each agency must ensure that only authorized change implementers are granted only least privileged access to information system components to implement the CAB-approved system changes or upgrades.

4.8. Post Change Validation

Each Agency Change Initiator/Owner must ensure that each system change outcome (successful or unsuccessful) is documented and that each change was implemented per the CAB-approved system change.

4.9. Auditing of System Changes

Each agency in consultation with the OCTO Change Manager must conduct a monthly audit to detect and resolve unapproved system changes.

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 in the *Policy Definitions website*.