Access Control Policy

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

1. Purpose

Specify requirements for minimizing risks of unauthorized access to the District of Columbia Government's (District) Systems and resources.

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.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 entity who receives any enterprise services from OCTO. In addition, this policy applies to any provider and third-party entity with access to District information, systems, networks, and/or 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 changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Account Management

District agencies must:

4.1.1. Identify and select the following types of system accounts to support the agency's missions/business functions:

- Administrator
- Standard
- Guest

4.1.2. Assign account managers for system accounts.

4.1.3. Establish conditions for group and role membership.

4.1.4. Specify authorized users of the system, group and role membership, access authorizations, and other attributes for each account.

4.1.5. Require approvals by organization-defined personnel or roles, for requests to create system accounts.

4.1.6. Create, enable, modify, disable, and remove system accounts by following the Access Control Procedures or by establishing agency-level account management procedures.

4.1.7. Monitor system account usage.

4.1.8. Notify account managers:

- When accounts are no longer required
- When users are separated or transferred; and
- When individual system usage or need-to-know changes

4.1.9. Authorize access to the system based on:

- Valid access authorizations
- Intended system usage; and
- Other attributes as required by the organization or associated missions/business functions

4.1.10. Review accounts for compliance with account management requirements at least annually.

4.1.11. Align account management processes with personnel separation and transfer processes.

4.2. Access Enforcement

Access to the District's sensitive information must be based upon a valid access authorization and intended system usage.

4.3. Separation of Duties

District agencies must:

4.3.1. Separate the roles and responsibilities to ensure that system administration and system auditing roles are not performed by the same personnel.

4.3.2. Document separation of duties of individuals; and

4.3.3. Define system access authorizations to support the separation of duties.

4.4. Least Privilege

District agencies must employ the concept of least privilege, allowing only authorized access for users only to accomplish assigned tasks and protect data according to classification outlined within the DC Data Policy.

4.5. Unsuccessful Login Attempts

District agencies information systems must:

4.5.1. Enforce a limit of 5 consecutive invalid login attempts by a user during a 2-hour period.

4.5.2. Automatically lock the account/node until released by an administrator when the maximum number of unsuccessful login attempts is exceeded.

4.6. System Use Notification

District agencies information systems must:

4.6.1. Before granting access to the system, display an agency approved logon banner containing the District approved wording that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance which states:

- User is accessing a District Government system
- System usage may be monitored, recorded, and subject to audit
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties
- Use of the system indicates consent to monitoring and recording

4.6.2. Retain the notification message on the screen until the user accepts the usage conditions and takes action to log on.

4.6.3. For publicly accessible systems:

- Display systems use information before granting further access
- Display references to monitoring, recording, or auditing that are consistent with privacy accommodations that generally prohibit those activities
- Describe the authorized uses of the system

4.7. Device Lock

District agencies information systems must:

4.7.1. Prevent system access by automatically initiating a device lock after 10 minutes of inactivity.

4.7.2. Retain the device lock until the user establishes access again using proper identification and authentication procedures.

4.7.3. During the period when a device is locked, conceal District information by displaying a publicly viewable image (e.g., District-approved screen savers, solid colors, blank screen, etc.).

4.8. Session Termination

District agencies' information systems must be configured to automatically terminate a user session after 10 minutes of inactivity or network disconnection.

4.9. Permitted Actions Without Identification or Authentication

District agencies must:

4.9.1. Identify agency user actions that can be performed on the system, without identification or authentication that is still consistent with the agency's mission, (e.g., access to District publicly available information, public websites, etc.).

4.9.2. Document and provide supporting evidence in the security plan for user actions not requiring identification or authentication.

4.10. Remote Access

District agencies must:

4.10.1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

4.10.2. Authorize remote access to the system before allowing such a connection.

4.10.3. Deploy the use of encrypted virtual private networks (VPNs) to enhance the confidentiality and integrity of remote connections (See *OCTO Virtual Private Network Policy*).

4.10.4. Access accounts used by remote vendors must only be enabled during the required period and must be disabled immediately thereafter.

4.10.5. Vendor accounts must be approved by the Agency's CIO or his/her designee and closely monitored.

4.10.6. Authorized third-party users must be required to authenticate before being allowed to access restricted information.

4.11. Wireless Access

District agencies must:

4.11.1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

4.11.2. Authorize wireless access to the system before allowing connections.

4.11.3. Protect wireless access to the system by deploying strong authentication of users and devices along with strong encryption that can reduce susceptibility to threats by adversaries involving wireless technologies.

4.12. Access Control for Mobile Devices

District agencies must:

4.12.1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

4.12.2. Authorize the connection of mobile devices to organizational systems.

4.12.3. Disable lock screen notifications on Mobile devices used for Multifactor Authentication (MFA) to ensure MFA codes cannot be seen without requiring a passcode to view.

4.13. Mobile Device Encryption

District agencies must employ appropriate encryption to protect the confidentiality and integrity of information on agency-approved mobile devices.

4.14. Use of External Systems

District agencies must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

4.14.1. Access any external systems.

4.14.2. Process, store, or transmit agency-specific information using external systems.

4.15. Publicly Accessible Content

District agencies must:

4.15.1. Designate individuals authorized to post information onto a publicly accessible system.

4.15.2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

4.15.3. Review the proposed content of information before posting onto the publicly accessible system to ensure that nonpublic information is not included.

4.15.4. Review the content on the publicly accessible system for nonpublic information on an annual basis and remove information, if discovered.

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*.