Identification and Authentication Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Review Date – 05/10/2024

1. Purpose

Establish the requirements for the identification and authentication of users, processes, or devices accessing the District of Columbia Government's (District) information system, and make sure that the security and integrity of the District data and information system are protected.

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.gov/us/dc/council/code/sections/1-1402.

3. Applicability

This policy applies to all data and records belonging to the District workforce members performing official functions on behalf of the District, and/or any entity who receive 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. Identification and Authentication | Organizational Users

The District agencies must ensure that organizational users or processes acting on behalf of organizational users are uniquely identified and authenticated before they are granted access (Local, Network or Remote) to the District information system's organizational users (or processes acting on behalf of organizational users).

4.2. Identification and Authentication |Multifactor Authentication to Privileged Accounts

All District agencies information systems must implement multifactor authentication for network access to privileged accounts.

4.3. Identification and Authentication |Multifactor Authentication to Non-Privileged Accounts

The District agencies must enforce the information system implements multi-factor authentication for network access to non-privileged accounts.

4.4. Identification and Authentication | Access to Accounts - Replay Resistant

The District Agencies must implement replay-resistant authentication mechanisms for access to privileged accounts, non-privileged accounts.

4.5. Identifier Management

The Districts agencies must manage information system identifiers by:

4.5.1. Receiving authorization from District workforce member's supervisor and agency management to assign an individual, group, role, or device identifier.

4.5.2. Selecting an identifier that identifies an individual, group, role, or device.

4.5.3. Assigning the identifier to the intended individual, group, role, or device.

4.5.4. Preventing reuse of identifiers for 7 years.

4.5.5. Disabling the identifier after 6 months of inactivity.

4.6. Authenticator Management

The District agencies must have Information system authentication requirements that are developed and properly managed. Individual authenticators including passwords, tokens, biometrics, PKI certificates, and key cards must be properly secured with the establishment of a secured log-on process to minimize the risk of unauthorized access.

The District agencies must manage information system authenticators by:

4.6.1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

4.6.2. Establishing initial authenticator content for authenticators defined by the organization.

4.6.3. Ensuring that authenticators have sufficient strength of mechanism for their intended use.

4.6.4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

4.6.5. Changing default content of authenticators before information system installation.

4.6.6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.

4.6.7. Changing/refreshing authenticators for group or role when membership to those accounts change (e.g., employee termination, transfer, etc.).

4.6.8. Protecting authenticator content from unauthorized disclosure and modification.

4.6.9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.

4.6.10. Changing authenticators for group/role accounts when membership to those accounts' changes.

4.7. Authenticator Management | Password-Based Authentication

The District agencies must enforce minimum password complexity as defined in the District: Password Management Policy.

4.8. Authenticator Feedback

The information system obscures feedback of authentication information during the authentication process to protect it from possible exploitation/use by unauthorized individuals.

4.9. Cryptographic Module Authentication

The District agencies must implement mechanisms for authentication to a cryptographic module (i.e., hardware or software device or component that performs cryptographic operations securely within a physical or logical boundary) that meets the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

4.10. Identification And Authentication | Non-Organizational Users

The District agencies must manage the information system that uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

4.11. Identification And Authentication | Acceptance of External Credentials

The District agencies must manage the information system to accept only external credentials that are certified to be compliant with the requirements of the NIST SP 800-63-3 (Digital Identity Guidelines).

4.12. Re-authentication

The District agencies must require users to re-authenticate to logically access the District systems in any of the following circumstances or as determined by the agency:

- System lock
- Role change
- After system upgrade/update
- To execute privileged functions
- To access sensitive data

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.*