|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Identification and Authentication** | **Updated:** 10/29/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of this Identification and Authentication policy is to establish a framework that ensures only authorized users and devices can access Information Technology (IT) resources. By implementing robust identification and authentication mechanisms, we aim to protect sensitive data and critical systems from unauthorized access, which can lead to data breaches, financial losses, and damage to the organization's reputation.

The benefits of this Identification and Authentication policy include enhanced security by minimizing unauthorized access, ensuring regulatory compliance to meet legal data protection requirements, and promoting accountability through traceable user actions. Additionally, it fosters user confidence in the protection of sensitive information, streamlines operational efficiency by clearly defining access roles, and allows for adaptability in updating methods to address emerging threats. Overall, this policy strengthens the organization’s cybersecurity posture and cultivates a culture of security awareness among users.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Identification and Authentication Policy ensures that all users and devices accessing the organization's information systems are uniquely identified and authenticated through multifactor authentication for both privileged and non-privileged accounts. It mandates the authentication of devices before network connection, effective management of identifiers, and strong password policies, including complexity and length requirements. The policy also requires obscured authentication feedback to protect against exploitation and compliance with legal standards for cryptographic module authentication.

* 1. Identification and Authentication

The [Owner] shall:

1. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of [Organization Name] users.
2. Ensure that information systems implement multifactor authentication for network access to privileged accounts.
3. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.
4. Ensure that information systems implement multifactor authentication for local access to privileged accounts.
5. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.
6. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.
7. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.
   1. Device Identification and Authentication

The [Owner] shall ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

* 1. Identifier Management

The [Owner] shall:

1. Ensure that the [Organization Name] manages information system identifiers by receiving authorization from [Owner] to assign an individual, group, role, or device identifier.
2. Select an identifier that identifies an individual, group, role, or device.
3. Assign the identifier to the intended individual, group, role, or device.
4. Prevent reuse of identifiers for 90 days.
5. Disable the identifier after 30 days of inactivity.
   1. Authentication Management

The [Owner] shall:

1. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
2. Establish initial authenticator content for authenticators defined by the organization.
3. Ensure that authenticators have sufficient strength of mechanism for their intended use.
4. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
5. Change default content of authenticators prior to information system installation.
6. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.
7. Change/refresh authenticators every 90 days.
8. Protect authenticator content from unauthorized disclosure and modification.
9. Require individuals and devices to implement specific security safeguards to protect authenticators.
10. Change authenticators for group/role accounts when membership to those account changes.
11. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.
12. Ensure passwords must contain characters from three of the following five categories:
    1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
    2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
    3. Base 10 digits (0 through 9);
    4. Non-alphanumeric characters ~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/; and
    5. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
13. Require passwords to have a minimum length of 8 characters.
14. Enforce at least one changed character when new passwords are created.
15. Store and transmit only cryptographically-protected passwords.
16. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.
17. Prohibit password reuse for 12 generations.
18. Allow the use of a temporary password for system logons with an immediate change to a permanent password.
19. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
20. Enforce authorized access to the corresponding private key.
21. Map the authenticated identity to the account of the individual or group.
22. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
23. Require that the registration process to receive [entity defined types of and/or specific authenticators] be conducted in person or by a trusted third party before [entity defined registration authority] with authorization by [entity defined personnel or roles].
24. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [entity defined token quality requirements].
    1. Authentication Feedback

The [Owner] shall: ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

* 1. Cryptographic Module Authentication

The [Owner] shall: Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

* 1. Cryptographic Module Authentication

The [Owner] shall:

1. Ensure that information systems uniquely identify and authenticate non-entity users or processes acting on behalf of non-entity users.
2. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.
3. Ensure that information systems accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.
4. Ensure that the organization employs only FICAM-approved information system components in [entity defined information systems] to accept third-party credentials.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-50 – Building a Cybersecurity and Privacy Learning Program](https://csrc.nist.gov/pubs/sp/800/50/r1/final)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-84 – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](https://csrc.nist.gov/pubs/sp/800/84/final)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-12 – An Introduction to Information Security](https://csrc.nist.gov/pubs/sp/800/12/r1/final)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-63 – Digital Identity Guidelines](https://pages.nist.gov/800-63-4/)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-73 – Interfaces for Personal Identity Verification: Part 3 – PIV Client Application Programming Interface](https://csrc.nist.gov/pubs/sp/800/73/pt3/5/final)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-76 – Biometric Specifications for Personal Identity Verification](https://csrc.nist.gov/pubs/sp/800/76/2/final)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-78 – Cryptographic Algorithms and Key Sizes for Personal Identity Verification](https://csrc.nist.gov/pubs/sp/800/78/5/final)

[National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-116 – Guidelines for the Use of PIV Credentials in Facility Access](https://csrc.nist.gov/pubs/sp/800/116/r1/final)