Insert Logo Here

Organization Name

Security Policy

Identification & Authentication

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published IA Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593090)

[2 Purpose 1](#_Toc68593091)

[3 Scope 1](#_Toc68593092)

[4 Roles and Responsibilities 1](#_Toc68593093)

[5 Management Commitment 2](#_Toc68593094)

[6 Authority 3](#_Toc68593095)

[7 Compliance 3](#_Toc68593096)

[8 Policy Requirements 4](#_Toc68593097)

[8.1 Identification And Authentication Policies and Procedures 4](#_Toc68593098)

[8.2 Identification and Authentication (Organizational Users) 4](#_Toc68593099)

[8.3 Device Identification And Authentication 4](#_Toc68593100)

[8.4 Identifier management 5](#_Toc68593101)

[8.5 Authenticator Management 5](#_Toc68593102)

[8.6 Authenticator Feedback 6](#_Toc68593103)

[8.7 Cryptographic Module Authentication 7](#_Toc68593104)

[8.8 Identification and Authentication (Non-Organizational Users) 7](#_Toc68593105)

# Introduction

Organization Name has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by Organization Name management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of Organization Name systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for Organization Name information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization Name and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization Name Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is Organization Name policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following identification and authentication requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the Organization Name information systems.

## Identification And Authentication Policies and Procedures

1. This document is intended to serve as the *Identification and Authorization Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Identification and Authorization Policy* and related controls have been developed, documented, and disseminated to all applicable personnel.
2. The Information Owner will review and update the *Identification and Authorization Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Identification and Authorization Policy* and/or procedure(s) must be sent to the Information Owner.

## Identification and Authentication (Organizational Users)

1. The following measures are implemented and maintained in the information system to identify and authenticate all organizational users of the system:

* A unique identifier and authentication are required for all privileged and non-privileged organizational users, including employees, contractors, guests, and processes acting on behalf of organizational users
* Multifactor authentication (MFA) is required for network access to privileged and non-privileged accounts and for local access to privileged accounts
* The MFA mechanism is replay-resistant
* When a group authenticator is employed, individuals are required to authenticate with their own unique authenticator
* MFA is required 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 meets the strength of mechanism requirements such as a soft token on mobile devices
* The system accepts and electronically verifies Personal Identity Verification (PIV) credentials for customer access

## Device Identification And Authentication

Organization Name must ensure that the information system uniquely identifies and authenticates any hardware device that accesses the information system before establishing a remote/network connection.

## Identifier management

1. Organization Name shall manage the information system identifiers for individual users and devices by:

* Receiving authorization from the ISSO to assign an individual, group, role, or device identifier
* Selecting an identifier that identifies an individual, group, role, or device
* Assigning the identifier to the intended individual, group, role, or device
* Preventing reuse of identifiers for at least 2 years
* Disabling the identifier after 90 days of inactivity
* Identifying individuals as contractors and foreign nationals

## Authenticator Management

1. Organization Name must manage information authenticators by:

* Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator
* Ensuring initial authenticator content for authenticators follow the policy established in this document
* Ensuring authenticators have sufficient strength of mechanism for their intended use
* Following the documented administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators
* Requiring default content of authenticators be changed upon initial login or information system installation
* Enforcing minimum and maximum lifetime restrictions and reuse conditions for authenticators
* Requiring and technically enforcing authenticators to be changed/refreshed at least every 60 days
* Implementing appropriate protection mechanisms to prevent authenticator content from being subject to unauthorized disclosure and modification
* Requiring users to take, and having devices implement, specific measures to safeguard authenticators
* Changing authenticators for group/role accounts when membership to those accounts’ changes
* Ensure that password-based authentication:
  + Enforces minimum password complexity of case sensitive, minimum of eight (8) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters
  + Enforces at least and (1) changed character when new passwords are created
  + Encrypts passwords in storage and in transmission
    - Passwords must be salted and hashed using a Password-based Key Derivation Function 2 (PBKDF2) that uses an approved one-way function such as Keyed Hash Message Authentication Code (HMAC), CMAC, or KMAC
    - The encrypted hash must be created using a FIPS-validated cryptographic module. The salt must be at least thirty two (32) bits in length and chosen arbitrarily so as to minimize salt value collisions among stored hashes
  + Enforces password minimum and maximum lifetime restrictions of one (1) day minimum and a sixty (60) day maximum
  + Prohibits password reuse for twenty four (24) generations
  + Allows the use of a temporary password for system logons with an immediate change to a permanent password
* Ensure that PKI-based authentication:
  + Validates certificates by constructing a certification path with status information to an accepted trust anchor
  + Enforces authorized access to the corresponding private key
  + Maps the authenticated identity to the user account of the individual or group
  + Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network
* Require that if hardware/biometric MFA tokens are used:
  + The registration process to receive the hardware/biometric tokens be carried out in person or by phone using corporate directory information before a designated registration authority with authorization by a designated organizational official (e.g. a supervisor)
  + Information employs mechanisms that satisfy token quality requirements for hardware token-based authentication.
* Employ automated tools to determine if password authenticators are sufficiently strong to satisfy complexity
* Protect authenticators commensurate with the security category of the information to which the authenticator permits access
* Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys

## Authenticator Feedback

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

## Cryptographic Module Authentication

The information system requires mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.