Insert Logo Here

Organization Name

Security Procedure

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 Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68606085)

[2 Purpose 1](#_Toc68606086)

[3 Scope 1](#_Toc68606087)

[4 Roles and Responsibilities 1](#_Toc68606088)

[5 Management Commitment 2](#_Toc68606089)

[6 Authority 3](#_Toc68606090)

[7 Compliance 3](#_Toc68606091)

[8 Procedural Requirements 4](#_Toc68606092)

[8.1 Unique User Access 4](#_Toc68606093)

[8.2 Authenticator Management 4](#_Toc68606094)

[8.3 Initial Authenticator Content 4](#_Toc68606095)

[8.4 Lost/Compromised & Revoking Authenticators 4](#_Toc68606096)

[8.5 Identifier Management 5](#_Toc68606097)

[8.6 Authenticator Content 5](#_Toc68606098)

[8.6.1 Information system (internal Active Directory) 5](#_Toc68606099)

[8.6.2 {Tool} (web application authentication) 6](#_Toc68606100)

[8.6.3 {Tool} Remote access 6](#_Toc68606101)

[8.7 Use of Authenticator Content 6](#_Toc68606102)

[8.8 PKI Based Authentication 7](#_Toc68606103)

[8.9 Authenticator FeedBack 7](#_Toc68606104)

[8.10 Cryptographic Module Authenticator 7](#_Toc68606105)

# Introduction

Organization Name has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures 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

This document defines the information identification and authentication procedures. These procedures are in place to facilitate the implementation of the Identification and Authentication Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# 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 procedures 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.

# Procedural 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.

## Unique User Access

All information users must be uniquely identified within the information system. The information system uses the following solution(s) and techniques to enforce unique identification and authentication:

* {Type of Account / Tool to enforce}
* {Type of Account / Tool to enforce}
* {Type of Account / Tool to enforce}

All accounts require Multifactor Authentication (MFA) and enforcement and group membership are managed via {Tool}. Multifactor authentication techniques are implemented and required for access to remote access to privileged accounts.

The information system {does/does not} use the Personal Identity Verification (PIV) credentials for Organization Name administrative personnel authentication. {Tool} provides PIV functionality to government clients if required.

## Authenticator Management

It is the client’s responsibility to provide the necessary interconnection requirements for SAML SSO via {Tool} for all user identifiers that require PIV or FICAM authentication.

## Initial Authenticator Content

Organization Name must verify the identity of the individual or device receiving authenticator content and users must confirm the employee’s uniquely identifiable username.

Initial authenticator content must also be configured so that users are assigned a random temporary password which meets password complexity requirements and requires a change at first use.

Authenticator content must be configured for sufficient strength so that user authenticator content meets TLS 1.2 encryption and cryptographic requirements by default. Authenticator content must be distributed so that initial user authentication is protected. If applicable, default authenticator content must be changed for any new system components, network devices, or application features.

## Lost/Compromised & Revoking Authenticators

Organization Name shall ensure authenticators are changed or refreshed at least every forty-five (45) days. In the event an authenticator has been lost or compromised, the user should contact the {Role/Team} immediately. Upon notification of a lost or compromised authenticator, the {Role/Team} will notify the {Role/Team}.

The {Role/Team} will disable the account if needed and/or assign the user a new authenticator.If the authenticator needs to be revoked, the {Role/Team} will immediately disable the account or revoke the credential from the specified user.

In order to maintain authenticator integrity and security, the information system will require:

* A minimum authenticator lifetime of one (1) days
* A maximum authenticator lifetime of forty-five (45) days
* Reuse conditions of twenty-four (24)

For all authenticator content Organization Name must instruct users on how to protect and safeguard authentication content from unauthorized disclosure or modification. As a rule, users must not:

* Write down passwords.
* Share passwords with anyone.
* Store passwords on unencrypted and unprotected systems.

Organization Name will require security safeguards specifically to protect authenticators and change authenticators for role based accounts. The information system will uniquely identify and authenticate, through Multi-Factor Authentication, individual system administrator user accounts before establishing a secure connection to the boundary. Additionally, VPN requires a {client certificate/other} on the member system to access the VPN.

## Identifier Management

The information system will uniquely identify contractors and foreign nationals that have access to the system within {Tool}. They will be identified by [placing a CT for contractors and FN for foreign nationals or other defined measures of identification]. The information system shall manage identifiers for users by:

* Utilizing the Account Request process to receive authorization from authorizing parties to determine who will be assigned a user identifier.
* Selecting an identifier that uniquely identifies an individual.
* Ensuring a process to assign the identifier to the intended user is developed and maintained.
* Preventing the reuse of identifiers for at least two years.
* Disabling the user identifier after ninety (90) days of inactivity.

## Authenticator Content

Password authentication must be enforced for the following systems, network devices, and application components and meet the following password criteria:

### Information system (internal Active Directory)

The information system internal {Tool} is the central domain controller and requires:

* Minimum of twelve (12) characters
* Windows password complexity requirements are enabled
* A minimum of at least one (1) character to be changed when new passwords are created
* Minimum of one (1) day lifetime restriction and a maximum lifetime of forty-five (45 days
* Prohibition of the last twenty-four (24) passwords used
* Feedback of authenticator content is configured to display masked characters
* Allows the use of a temporary password for system logons with an immediate change to the password

### {Tool} (web application authentication)

{Tool} , the web application authentication requires:

* Minimum of seven (7) characters
* At least one (1) upper case, one (1) lower case, and one (1) number
* A minimum of at least one (1) character to be changed when new passwords are created
* Minimum of one (1) day lifetime restriction and a maximum lifetime of sixty (60) days
* Prohibition of the last twenty-four (24) passwords used
* Feedback of authenticator content must be configured to display masked characters
* Allows the use of a temporary password for system logons with an immediate change to the password

### {Tool} Remote access

{Tool} authentication requires:

* Two-factor authentication
* Minimum of fourteen (14) characters
* Windows password complexity requirements are enabled
* A minimum of at least one (1) character to be changed when new passwords are created
* Minimum of one (1) day lifetime restriction and a maximum lifetime of sixty (45) days
* Prohibition of the last twenty-four (24) passwords used
* Feedback of authenticator content must be configured to display masked characters
* Allows the use of a temporary password for system logons with an immediate change to the password

## Use of Authenticator Content

Organization Name {does/does not} use smart cards to access or manage the information SaaS. Password policies are employed to ensure that authenticators sufficiently satisfy the password requirements. Any passwords that do not meet the requirements will prompt users to re-enter a satisfactory password. Users will not be allowed to resume normal functions until a sufficient password has been used.

All passwords are to be considered confidential and are stored and transmitted using Validated encryption. Unencrypted static authenticators {are/are not} used within the information system. Embedded authenticators {are/are not} used for access to services or resources and there {are/are not} stored functions used in the operation of the system or within the application. Authenticators to access services or resources are accessed via procedure calls to {Tool}.

## PKI Based Authentication

Organization Name {does/does not} use PKI to access or manage the information system.

## Authenticator FeedBack

Organization Name will employ controls to obscure passwords from unauthorized individuals through masking. In the event of invalid login, the system informs the user that login was unsuccessful, but does not provide any information that might compromise the authentication mechanism, as outlined in the following related policies and procedures.

## Cryptographic Module Authenticator

Organization Name publicly available web applications {do/do not} contain sensitive data. Access to internet facing web applications involving sensitive information is protected using approved levels of encryption at a minimum.

The web application and all relevant data presented in the web session is encrypted through digital certificates as it is transmitted via the Internet and within the system environment. All encryption methods used are validated and all systems, as appropriate have, at a minimum, TLS 1.2 and/or AES 128-bit encryption.