

{Insert CompanY Name}

Security Procedures

Identification and Authentication [IA]

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Procedural Requirements [IA-1] .............................................................................................................. 4

8.1 User Identification and Authentication [IA-2] .................................................................................. 4

8.2 Device Identification and Authentication [IA-3] ............................................................................... 4

8.3 Identifier Management [IA-4] .......................................................................................................... 4

8.4 Authenticator Management [IA-5] ................................................................................................... 5

8.4.1 Initial Authenticator Content and Distribution ........................................................................... 5

8.4.2 Authenticator Strength and Maximum Lifetime ........................................................................ 6

8.4.3 Lost/Compromised & Revoking Authenticators ......................................................................... 6

8.4.4 Default Authentication Content ................................................................................................. 6

8.4.5 Authenticator Restrictions and Reuse ........................................................................................ 7

8.4.6 Protecting Authenticators from Unauthorized Disclosure ......................................................... 8

8.4.7 Authenticator Assessments ........................................................................................................ 8

8.4.8 Authenticator Storage and Transmission ................................................................................... 9

8.4.9 Public Key-Based Authentication ................................................................................................ 9

8.5 Authenticator Feedback [IA-6] ....................................................................................................... 10

8.6 Cryptographic Module Authenticator [IA-7] .................................................................................. 10

8.7 Identification and Authentication (Non-Organizational Users) [IA-8]] .......................................... 10

8.8 Re-authentication] IA-11] ............................................................................................................... 10

8.9 Identity Proofing [IA-12] ................................................................................................................. 10

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s 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 5.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s 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 {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **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 {Insert Company 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | 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 Director | 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 Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company 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 {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company 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
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. 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 {Insert Company Name}’s 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 by an external vendor and/or internal self-assessments 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 [IA-1]

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 {Insert Company Name} information systems.

8.1 User Identification and Authentication [IA-2]

All information users, including privileged and non-privileged, are uniquely identified within the {Insert Product Name} Information System. The information system uses the following solution(s) and techniques to enforce unique identification and authentication: [IA-2]

* Administrator accounts for {Insert Vendor(s) Name} access through {Insert Documentation Repository Name} are uniquely identified. Administrator accounts have a suffix of {Insert Organizational Language} for IT Team members and {Insert Organizational Language} for Information Security Team members. This nomenclature applies to both {Insert Documentation Repository Name}, which is used to uniquely identify back-end administrators who access {Insert Vendor(s) Name} resources via {Insert Vendor(s) Name}, and the corporate {Insert Documentation Repository Name}, which is used to manage permissions for administrators configuring infrastructure resources.
* {Insert Documentation Repository} accounts are assigned to individuals with a unique username.
* {Insert Vendor(s) Name} is used to uniquely identify {Insert Product Name} users and administrators accessing the {Insert Product Name} Application.

{Insert Company Name} considers all access to the backend {Insert Product Name} Infrastructure as privileged access and has implemented required multifactor authentication mechanisms for network access to {Insert Product Name} with {Insert Documentation Repository Name} and {Insert MFA Device Name}. Access to the web portal for privileged and non-privileged accounts has multifactor authentication available via {Insert Vendor(s) Name} along with SAML SSO for government clients. These multifactor authentication options adhere to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL), and are phishing-resistant. [IA-2 (1)] [IA-2 (2)] Access to {Insert Product Name} is granted only to authorized {Insert Company Name} personnel based on separation of duties and least privilege principles. Remote access to the {Insert Product Name} Infrastructure is limited to the {Insert application or device(s) Name}, {Insert Company Name}’s jump servers, and the {Insert Vendor(s) Name}. {Insert MFA Device(s) Name} and {Insert Vendor(s) Name} are both factors of authentication that are separate from the {Insert Product Name} Information System. [IA-2 (6) (a)]

MFA is required for local, network, and remote access to the {Insert Product Name} Information System for privileged and non-privileged accounts. [IA-2 (6)] {Insert MFA Device(s) Name} and {Insert Validation Application Name} providing MFA utilize FIPS validated or NSA approved cryptography. [IA-2 (6) (b)]

{Insert Company Name} prohibits the use of group/shared accounts and authenticators within the {Insert Product Name} Information System. All access to the {Insert Product Name} Information System is configured to use unique identifiers and authenticators. [IA-2 (5)]

{Insert Company Name} has configured {Insert Product Name} to utilize several replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. [IA-2 (8)] {Insert Company Name} has configured the {Insert Vendor(s) Name} to require {Insert MFA Device Name} MFA for every authentication attempt. {Insert Product Name} utilizes {Insert Documentation Repository Name} for {Insert Vendor(s) Name} authentication which uses Kerberos to protect against replay attacks. Additionally, the {Insert Product Name} utilizes TLS 1.2 with hardened cipher suites which protect against replay attacks.

The {Insert Product Name} Information System does not use the Personal Identity Verification (PIV) credentials for {Insert Company Name} administrative personnel authentication. The {Insert Product Name} has been configured to provide government customers the capability to integrate their existing PIV or CAC solution with the {Insert Product Name} through federation with their organizational directory and authentication management mechanism to achieve full compliance with program authentication requirements. [IA-2 (12)]

8.2 Device Identification and Authentication [IA-3]

{Insert Company Name} ensures that the {Insert Product Name} Information System uniquely identifies and authenticates any hardware device that accesses the information system before establishing a local, remote, or network connection via computer accounts in {Insert Documentation Repository Name}. The {Insert Product Name} uniquely identifies devices connecting to the web application by recording the MAC address and the IP address of the device.

8.3 Identifier Management [IA-4]

Access to the {Insert Product Name} Information System is restricted to authorized {Insert Company Name} personnel. Granting access to the {Insert Product Name} Information System follows the account management process. {Insert Company Name} personnel must submit an access request through the {Insert Company Name} {Insert Documentation Repository Name} Request Form that includes the type of access being requested and the reason why this access is necessary. The {Insert Product Name} Information Security Manager and Product Owner must authorize all privileged {Insert Product Name} Application access requests and document their authorization in {Insert Documentation Repository Name}. [IA-4 (a)] The {Insert Product Name} Information Security Manager and Information Technology Manager must authorize all backend {Insert Product Name} Infrastructure access requests and document their authorization in {Insert Documentation Ticketing Repository Name}. All approved logical access to the {Insert Product Name} Information System is enforced by either {Insert Documentation Repository Name}, {Insert Documentation Repository Name}, or {Insert Documentation Repository Name}.

{Insert Company Name} selects identifiers that uniquely identify the individual assigned to the account and follow a {Organizationally Defined} naming convention. [IA-4 (b] [IA-4 (c)] Identifiers are not assigned to an individual unless authorization is received from the Information Security Manager.

{Insert Documentation Repository Name} and {Insert Documentation Repository Name} are used to uniquely identify users across the {Insert Product Name} Information System. {Insert Company Name} administrator personnel manage {Insert Product Name} Information System authenticators. {Insert Company Name} personnel who are authorized to access the {Insert Product Name} Information System are responsible for creating, securing, and using strong authenticators that adhere to authenticator management requirements.

{Insert Company Name} prevents the reuse of identifiers for at least two (2) years through configuration settings in {Insert Documentation Repository Name}. [IA-4 (d)] {Insert Company Name} implements automated mechanisms through {Insert Documentation Repository Name} and {Insert SIEM} to disable identifiers after ninety (90) days of inactivity.

The {Insert Company Name} Identification and Authentication policy {Insert Organization Define Control language for foreign national and 3rd party} from accessing the {Insert Product Name} Information System. However, if {Insert Company Name} did use contractors or foreign nationals, the {Insert Product Name} account identifiers would designate their disposition accordingly as a contractor or foreign national {Insert Organization Defined Naming Convention} suffix in their username. [IA-4 (4)]

8.4 Authenticator Management [IA-5]

#### Initial Authenticator Content and Distribution

All personnel requiring administrative access to the {Insert Vendor(s) Name}, servers, or network components supporting the {Insert Product Name} Information System must be an authorized member of the {Insert Company Name} IT, Information Security, or Development team.

During the onboarding process, new {Insert Product Name} administrator and {Insert Vendor(s) Name} Identity and Access Management (IAM) account unique user identifiers are requested and approved via the {Insert Documentation Repository Name} process flow. [IA-5 (b)] Unique user identifiers are communicated to the user either directly or via {Insert Organization Specific Notification Method} to verify the identity of the individual. [IA-5 (a)] [IA-5 (d)] {{Leave if applicable} This communication includes additional instructions to set up MFA on their account.} Authenticators for all {Insert Product Name} internal administrative accounts require users to change their initial authenticator content upon first login. [IA-5 (e)]

{Insert Company Name} {Insert Organizationally Defined Control Language} the use of group accounts within the {Insert Product Name} Information System for internal personnel and systems. [IA-5 (I)] It is the responsibility of the Client or Vendor to make the decision to allow group accounts and the responsibility of the Client or Vendor to manage the authenticators for these accounts.

#### Authenticator Strength and Maximum Lifetime

{Insert Company Name} has configured the {Insert Product Name} Information System password policies to ensure that strong passwords are enforced for all privileged and non-privileged accounts. [IA-5 (1) (c)] Strong {Insert OS Name} passwords contain characters from at least three of the following categories:

{Modify list below, per organization requirements}

* Uppercase letters
* Lowercase letters
* Base 10 digits (0 through 9)
* Special characters such as:
  + ~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/
* Any Unicode character that is categorized as an alphabetic character, but it is not uppercase or lowercase (such as Unicode characters from Asian languages).

Password authentication is enforced for the following systems, network devices, and application components and meet the password criteria as detailed in the sections below.

##### {Insert Product Name} Information System

The directory service within the {Insert Product Name} Information System is {Insert Documentation Repository Name} and requires:

{Modify list below, per organization requirements}

* Minimum of fourteen (14) characters
* {Insert OS Name} password complexity requirements are enabled [IA-5 (1) (h)]
* 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 [IA-5 (1) (e)]
* Allows the following symbols: "!#$%&’()\*+,-./\:;<=>?@[]^`{|}~ [IA-5 (1) (f)]

##### {Insert Product Name} Authentication

{Insert Product Name}, the web application authentication, is the universal directory and requires:

{Modify list below, per organization requirements}

* 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
* Allows the selection of long passwords and passphrases, including spaces and all printable characters [IA-5 (1) (f)]

##### Remote access

{Modify list below, per organization requirements}

* Remote access to the {Insert Product Name} Information System is through {Insert Vendor(s) Name}. {Insert Vendor(s) Name} requires authentication to {Insert Vendor(s) Name}. {Insert Vendor(s) Name} authentication requires:
* Two-factor authentication
* Minimum of fourteen (14) characters
* {Insert OS Name} password complexity requirements are enabled [IA-5 (1) (h)]
* 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 must be configured to display masked characters
* Allows for the use of a temporary password for system logons and requires an immediate change to the password [IA-5 (1) (e)]
* Allows user selection of long passwords and passphrases, including spaces and all printable characters [IA-5 (1) (f)]

#### Lost/Compromised & Revoking Authenticators

In the event an authenticator has been lost or compromised, the user must contact the Information Technology Team immediately. Upon notification of a lost or compromised authenticator, the Information Technology Team will notify the Information Security Team.

The Information Technology Team will disable the account if needed and/or assign the user a new authenticator. If the authenticator needs to be revoked, the Information Technology Team will immediately disable the account or revoke the credential from the specified user. The Information Security Team will review events associated with the lost or compromised credential.

In the event a multifactor authentication device is lost or needs to be revoked for any reason, the Information Technology Team will revoke the account authenticator in {Insert Documentation Repository Name} or {Insert SIEM Name} and prompt the user to set up a new MFA device if the individual still requires access. [IA-5 (d)]

#### Default Authentication Content

For new {Insert SIEM Name} accounts, an initial password is provided by {Insert Product Name} administrator personnel to the new administrator users for their account, which they must change upon first login. To reduce the potential for lost or stolen credentials to the {Insert Product Name} production resources, {Insert Vendor(s) Name} secret access keys are not provided to administrator personnel as part of the provisioning or password reset processes for {Insert Product Name} user accounts. Built in accounts within a new server are renamed and disabled and local password management is handled through the Local Administrator Password Solution (LAPS) in accordance with the DISA STIGs.

#### Authenticator Restrictions and Reuse

In order to maintain authenticator integrity and security, the {Insert Product Name} Information System requires:

{Modify list below, per organization requirements}

* A minimum authenticator lifetime of one (1) days
* A maximum authenticator lifetime of forty-five (45) days, and/or the authenticator has been lost, compromised, or damaged [IA-5 (f)]
* Prohibit reuse of the last twenty-four (24) passwords used

#### Protecting Authenticators from Unauthorized Disclosure

{Insert Company Name} requires that all personnel maintain personal accountability for practicing good and ethical security practices, which include at a minimum but are not limited to: [IA-5 (g)]

{Modify list below, per organization requirements}

* Maintaining the confidentiality of authentication codes and devices
* Not sharing passwords with other individuals
* Avoiding access by others to personal authentication codes and devices
* Not requesting others to share their personal authentication codes or devices
* Using authentication codes only for approved business purposes
* Notifying the Information Security team of any indication of possible compromise of an authentication device

Passwords are transmitted and stored in an encrypted state utilizing FIPS 140-2 approved algorithms.

{Insert Company Name} requires security safeguards specifically to protect authenticators and change authenticators for role accounts via Mobile Device Management (MDM). [IA-5 (h)] {Insert Company Name} has configured {Insert Vendor(s) Name} policies to require PIN or biometric based protections of mobile devices. [IA-5 (6)]

#### Authenticator Assessments

The {Insert Product Name} Information System password rules require strong passwords, and each access control mechanism automatically verifies that each user’s password meets the password policy. 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 compliant password has been used. Additionally, {Insert Company Name} leverages {Insert Vendor(s) Name} to conduct vulnerability scans and configuration checks against the {Insert Product Name} and the {Insert Product Name} Infrastructure.

{Insert Company Name} utilizes {Insert Vendor(s) Name} to monitor corporate administrator account passwords for weaknesses and vulnerabilities. {Insert Vendor(s) Name} does not have any access to see blank text passwords but only the password’s hash value. {Insert Vendor(s) Name} will compare this hash value to a database of known compromised and weak passwords and report accordingly. The Information Security Team monitors {Insert Vendor(s) Name} and will alert users to password weaknesses and vulnerabilities and ensure that the passwords are updated to be sufficiently strong and compliant. The {Insert Vendor(s) Name} which provides initial access to the {Insert Product Name} Information System is only accessible by using designated {Insert Organization Level Role} administrator accounts assigned to specific individuals. {(Leave if Applicable) {Insert Organization Control Language if N/A} Group and shared administrator accounts are prohibited. [IA-5 (1) (a)] [IA-5 (1) (b)]}

The {Insert Product Name} will automatically evaluate a user’s password and inform the user whether the password entered is strong enough for the application’s password strength, complexity, and history parameters. [IA-5 (1) (g)]

#### Authenticator Storage and Transmission

All passwords are considered confidential and are stored and transmitted using FIPS Validated encryption. [IA-5 (1) (c)] [IA-5 (1) (d)] Unencrypted static authenticators are not used within the information system. [IA-5 (7)] Embedded authenticators are not used for access to services or resources and there 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 {Insert Vendor(s) Name}.

#### Public Key-Based Authentication

For Infrastructure, {Insert Company Name} leverages the built in {Insert OS Name(s) e.g., Linux, Microsoft Windows, and Windows Active Directory} public key functionality to perform public key infrastructure authentication management. Including: [IA-5 (2)]

* Validation of certification paths to a trusted Certificate Authority [IA-5 (2) (b) (1)]
* Enforcement of authorized access to private keys [IA-5 (2) (a) (1)]
* Determination of the authenticated identity to the account of the individual or group [IA-5 (2) (a) (2)]
* Implementation of a local revocation data cache to support path discovery and validation [IA-5 (2) (b) (2)]

For the {Insert Product Name} Application, {Insert Company Name} leverages {Insert Vendor(s) Name} public key functionality to perform public key infrastructure authentication management. Including: [IA-5 (2)]

* Validation of certification paths to a trusted Certificate Authority [IA-5 (2) (b) (1)]
* Enforcement of authorized access to private keys [IA-5 (2) (a) (1)]
* Determination of the authenticated identity to the account of the individual or group [IA-5 (2) (a) (2)]
* Implementation of a local revocation data cache to support path discovery and validation [IA-5 (2) (b) (2)]

8.5 Authenticator Feedback [IA-6]

{Insert Company Name} employs controls to obscure passwords from unauthorized individuals through masking. The {Insert Role or Team Name} has configured the {Insert Product Name} to obscure passwords during logon sessions, which require users to enter a string of characters. Passwords are displayed as asterisks when typed in, so the content of the character string remains hidden. 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. [IA-6]

8.6 Cryptographic Module Authenticator [IA-7]

{Insert Company Name} {Leave only if applicable or write control language specific to organization} *publicly available web applications do not contain sensitive data. Access to internet facing web applications involving sensitive information is protected using approved, FIPS 140-2 level 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 FIPS 140-2 validated and all systems, as appropriate have, at a minimum, TLS 1.2 and/or AES 128-bit encryption. [IA-7]

8.7 Identification and Authentication (Non-Organizational Users) [IA-8]

{Insert Product Name} customer accounts utilize {Insert Vendor(s) Name} which requires a unique user ID, password, and MFA. [IA-8] The {Insert Product Name} has the ability to integrate with a customer’s single sign-on (SSO) through LDAP directories or OpenID identity federation. Agency customers who are required to use a hardware-based Personal Identity Verification (PIV) card or Common Access Card (CAC) can either utilize {Insert Vendor(s) Name} or work with {Insert Product Name} support to enable SSO capability within the {Insert Product Name} using identity federation through OpenID. [IA-8 (1)] [IA-8 (4)] [IA-8 (2) (b)] The {Insert Product Name} will only accept external authenticators that are NIST-compliant. [IA-8 (2) (a)]

8.8 Re-authentication] IA-11]

The {Insert Product Name} Information system is configured to require users to re-authenticate:

* When the device locks
* When a user changes roles
* After an extended period of 12 hours
* After 15 minutes of inactivity

8.9 Identity Proofing [IA-12]

During onboarding, the {Insert Company Name} Human Resources department performs the identity proofing as part of the I-9 employment eligibility verification process. New employees {Insert Organization Specific Process} and presented with their unique authentication credentials.

Customers are responsible for their own employee identity proofing for the {Insert Product Name}.