

{Insert Company Name}

Security Policy

Identification and Authentication

**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 Policy Requirements ................................................................................................................................ 4

8.1 Identification and Authentication Policies and Procedures [IA-1] ................................................... 4

8.2 Identification and Authentication (Organizational Users) [IA-2, IA-2 (1,2,5,6,8,12)] ....................... 4

8.3 Device Identification and Authentication [IA-3] ............................................................................... 5

8.4 Identifier Management [IA-4, IA-4 (4)] ............................................................................................. 5

8.5 Authenticator Management [IA-5, IA-5 (1,2,6,7), {IA-5 (8,13) High Only}] ...................................... 5

8.5.1 Public Key-Based Authentication .......................................................................................... 7

8.5.2 Protection of Authenticators ................................................................................................ 7

8.5.3 Multiple System Accounts and Expiration of Cached Authenticators ................................... 7

8.6 Authenticator Feedback [IA-6] ......................................................................................................... 7

8.7 Cryptographic Module Authentication [IA-7] ................................................................................... 7

8.8 Identification and Authentication (Non-Organizational Users) [IA-8, IA-8 (1,2,4)] .......................... 8

8.9 Re-Authentication [IA-11] ................................................................................................................ 8

8.10 Identity Proofing [IA-12, IA-12 (2,3,5), {IA-12 (4) High Only}] ........................................................ 8

# 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.

# Policy Requirements

The following personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company/Product Name} information systems.

8.1 Identification and Authentication Policies and Procedures [IA-1]

This document is intended to serve as the Identification and Authentication Policy and is made available

to all applicable personnel. The associated procedure(s) to facilitate the implementation of the

Identification and Authentication Policy and related controls have been developed, documented, and

disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief

privacy officer, ISSO, and/or similar roles or their designees: [IA-1 (a)]

* An organizational-level Identification and Authentication Policy that: [IA-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment,

coordination among organizational entities, and compliance [IA-1 (a) (1) (a)]

* + Is consistent with applicable laws, executive orders, directives, regulations, policies,

standards, and guidelines [IA-1 (a) (1) (b)]

* Procedures to facilitate the implementation of Identification and Authentication Policy and the

associated Identification and Authentication controls [IA-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the

development, documentation, and dissemination of the Identification and Authentication policy and

procedures. [IA-1 (b)]

{Insert Company Name} must review and update the current Identification and Authentication: [IA-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [IA-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [IA-1 (c) (2)]

8.2 Identification and Authentication (Organizational Users) [IA-2, IA-2 (1,2,5,6,8,12)]

The following measures must be implemented and maintained in {Insert Company Name} information systems to identify and authenticate all organizational users of the information systems:

* A unique identifier and authentication must be required for all privileged and non-privileged organizational users, including employees, contractors, guests, and processes acting on behalf of organizational users [IA-2]
* Multifactor authentication (MFA) must be required for access to privileged and non-privileged accounts. For systems hosting Federal or State government data, MFA must be configured in accordance with SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL) [IA-2 (1, 2)]
* Multi-factor authentication must be phishing-resistant [IA-2 (1)]
* When shared accounts or authenticators are employed, users must be required to authenticate with their own unique authenticator prior to granting access to the shared accounts or resources [IA-2 (5)]
* MFA must be required for local, network, and remote access to privileged and non-privileged accounts [IA-2 (6)]
  + One of the factors must be provided by a device separate from the system gaining access. [IA-2 (6) (a)] Examples include soft token on mobile device or a smart card such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card
  + For systems storing or processing Federal government information, the device must utilize FIPS validated or NSA approved cryptography (see SC-13) [IA-2 (6) (b)]
* The MFA mechanism must be replay-resistant for privileged and non-privileged accounts [IA-2 (8)]
* For systems storing or processing Federal government information, the information system must accept and electronically verify Personal Identity Verification (PIV) compliant credentials [IA-2 (12)]

8.3 Device Identification and Authentication [IA-3]

{Insert Company Name} must ensure that the information system uniquely identifies and authenticates any hardware device that accesses the information system before establishing a local, remote, or network connection.

8.4 Identifier Management [IA-4, IA-4 (4)]

{Insert Company Name} must manage information system identifiers for individual users and devices by: [IA-4]

* Receiving authorization from the System Owner, Information Security Manager (ISM) or ISSO to assign an individual, group, role, or device identifier [IA-4 (a)]
* Selecting an identifier that identifies an individual, group, role, service, or device [IA-4 (b)]
* Assigning the identifier to the intended individual, group, role, service, or device [IA-4 (c)]
* Preventing reuse of identifiers for at least two (2) years [IA-4 (d)]
* Uniquely identifying individuals as contractors and/or foreign nationals, as applicable [IA-4 (4)]

8.5 Authenticator Management [IA-5, IA-5 (1,2,6,7), {IA-5 (8,13) High Only}]

{Insert Company Name} must manage information system authenticators by: [IA-5]

* Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, and/or device receiving the authenticator. [IA-5 (a)]
  + For systems storing or processing Federal or State government information, the authenticator must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 3 for high impact systems, level 2 for moderate impact, and level 1 for low impact.
* Establishing initial authenticator content for any authenticators issued by the organization [IA-5 (b)]
* Ensuring authenticators have sufficient strength of mechanism for their intended use [IA-5 (c)]
  + For systems storing or processing Federal or State government information, {Insert Company Name} must follow NIST SP 800-63C Section 6.2.3 Encrypted Assertion which requires that authentication assertions be encrypted when passed through third parties
* Establishing and implementing administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators [IA-5 (d)]
* Changing default authenticators prior to first use [IA-5 (e)]
* Changing or refreshing authenticators at least every 60 days and/or if the authenticator has been lost, compromised, or damaged [IA-5 (f)]
* Implementing protection mechanisms to prevent authenticator content from being subject to unauthorized disclosure and modification [IA-5 (g)]
* Requiring users to take, and having devices implement, specific measures to safeguard authenticators [IA-5 (h)]
* Changing authenticators for group or role accounts when membership to those accounts changes [IA-5 (i)]

For password-based authentication, {Insert Company Name} must: [IA-5 (1)]

* Maintain a list of commonly used, expected, or compromised passwords and update the list at least yearly and when organizational passwords are suspected to have been directly or indirectly compromised [IA-5 (1) (a)]
* Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-5 (1) (a) [IA-5 (1) (b)]
* Transmit passwords only over cryptographically protected channels [IA-5 (1) (c)]
* Store passwords using an approved salted key derivation function, preferably using a keyed hash [IA-5 (1) (d)]
* Upon account recovery a new password is immediately required [IA-5 (1) (e)]
* Allow user selection of long passwords and passphrases, including spaces and all printable characters [IA-5 (1) (f)]
* Employ automated tools to assist the user in selecting strong password authenticators [IA-5 (1) (g)]
* Enforce composition and complexity rules commensurate with the security category of the information system [IA-5 (1) (h)]
  + For systems storing or processing Federal or State government information, the minimum requirements are:
    - Minimum of fourteen (14) characters
    - At least one (1) of each:
    - Upper-case letter
    - Lower-case letter
    - Number
    - Special character

### Public Key-based Authentication

{Insert Company Name} must ensure that public key-based authentication: [IA-5 (2) (a)]

* Enforces authorized access to the corresponding private key [IA-5 (2) (a) (1)]
* Maps the authenticated identity to the user account of the individual or group [IA-5 (2) (a) (2)]

When Public Key Infrastructure (PKI) is used, {Insert Company Name} must: [IA-5 (2) (b)]

* Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information [IA-5 (2) (b) (1)]
* Implement a local cache of revocation data to support path discovery and validation [IA-5 (2) (b) (2)]

### Protection of Authenticators

{Insert Company Name} must:

* Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access. [IA-5 (6)]
* Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage. [IA-5 (7)]

### Multiple System Accounts and Expiration of Cached Authenticators

**For high impact systems only:**

{Insert Company Name} must:

* Implement different authenticators in different user authentication domains to manage the risk of compromise due to individual having accounts on multiple systems. [IA-5 (8)]
* Prohibit the use of cached authenticators after 60 days. [IA-5 (13)]

8.6 Authenticator Feedback [IA-6]

{Insert Company Name} must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

8.7 Cryptographic Module Authentication [IA-7]

{Insert Company Name} must implement 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.

8.8 Identification and Authentication (Non-Organizational Users) [IA-8, IA-8 )1,2,4)]

{Insert Company Name} must:

* Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users. [IA-8]
* Document and maintain a list of accepted external authenticators. [IA-8 (2) (b)]
* For systems storing or processing Federal government information:
  + Accept and electronically verify Personal Identity Verification-compliant (PIV) credentials from other government agencies. [IA-8 (1)]
  + Accept only external authenticators that are NIST-compliant. [IA-8 (2) (a)]
  + Conform to Federal Identity, Credential, and Access Management (FICAM) issued profiles. [IA-8 (4)]

8.9 Re-Authentication [IA-11]

{Insert Company Name} requires users to re-authenticate when:

* The device locks,
* When the user changes roles,
* After an extended period of 12 hours, and
* After 15 minutes of inactivity on high impact systems, after 30 minutes of inactivity for all others.

8.10 Identity Proofing [IA-12, IA-12 (2,3,5), {IA-12 (4) High Only}]

{Insert Company Name} must: [IA-12]

* Identify proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines [IA-12 (a)]
* Resolve user identities to a unique individual [IA-12 (b)]
* Collect, validate, and verify identity evidence [IA-12 (c)]
* Require evidence of individual identification be presented to the registration authority. [IA-12 (2)]
* Require that the presented identity evidence be validated and verified through a method consistent with the risks to the systems, roles, and privileges associated with the user’s account [IA-12 (3)]
* Require that a notice of proofing or registration code be delivered through an out-of-band channel to verify the user’s physical or digital address of record. [IA-12 (5)]

**For high impact systems only:**

{Insert Company Name} must require that the validation and verification of identity evidence be conducted in person or a proctored video conference before a designated registration authority in accordance with NIST SP 800-63A Enrollment and Identity Proofing. [IA-12 (4)]