Insert Logo Here

Organization Name

Security Policy

Access Control

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 AC Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc60733286)

[2 Purpose 1](#_Toc60733287)

[3 Scope 1](#_Toc60733288)

[4 Roles and Responsibilities 1](#_Toc60733289)

[5 Management Commitment 2](#_Toc60733290)

[6 Authority 3](#_Toc60733291)

[7 Compliance 3](#_Toc60733292)

[8 Policy Requirements 4](#_Toc60733293)

[8.1 Access Control Policies and Procedures 4](#_Toc60733294)

[8.2 Account Management 4](#_Toc60733295)

[8.3 Access Enforcement 5](#_Toc60733296)

[8.4 Information Flow Enforcement 5](#_Toc60733297)

[8.5 Separation of Duties 5](#_Toc60733298)

[8.6 Least Privilege 5](#_Toc60733299)

[8.7 Unsuccessful Log in Attempts 6](#_Toc60733300)

[8.8 System Use Notifications 6](#_Toc60733301)

[8.9 Concurrent Sessions 6](#_Toc60733302)

[8.10 Session Lock and Termination 6](#_Toc60733303)

[8.11 Permitted Actions without Identification or Authentication 7](#_Toc60733304)

[8.12 Remote Access 7](#_Toc60733305)

[8.13 Wireless Access 7](#_Toc60733306)

[8.14 Access Control for Mobile Devices 7](#_Toc60733307)

[8.15 Use of External Information Systems and Information Sharing 7](#_Toc60733308)

[8.16 Publicly Accessible Content 8](#_Toc60733309)

# 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’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 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 access control 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.

## Access Control Policies and Procedures

This document is intended to serve as the *Access Control Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Access Control Policy* and related physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Access Control 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 *Access Control Policy* and/or procedure(s) must be sent to the Information Owner.

## Account Management

Organization Name has implemented and maintains an information system account management process intended to carry out the following activities:

1. Identify accounts necessary to support company mission and business functions including Individual, Group, System, Application, Guest/Anonymous, Temporary, and other accounts if they exist
2. Assign account managers for information system accounts
3. Establish conditions for group and role membership
4. Control information system access, employing group and role membership, access authorizations, and defined attributes for each account
5. Ensure all information system accounts require approval by defined personnel or roles
6. Maintain the capability to establish, activate, modify, disable, or remove accounts in accordance with defined policies and procedures
7. Monitor information system account users
8. Ensure mechanisms are implemented to notify account managers when accounts are no longer required, including when information system users are terminated transferred, or information system usage or need-to know/need-to-share changes
9. Grant information system access based on a valid access authorization, intended system usage, and company defined attributes
10. Ensure system accounts are reviewed annually
11. Employ a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group
12. Employ automated mechanisms to support in the management of information system accounts, including those identified in AC-2(a)
13. Have mechanisms in place to automatically remove or disable temporary and emergency accounts after no more than thirty (30) days
14. Automatically disable inactive accounts after ninety (90) days
15. Automatically audit and generates notifications to defined personnel or role based on account creations, account modifications, and disabling and terminating actions
16. Require users to log out when they expect to be away from their workstations for a defined period of time in accordance with a defined time period of expected inactivity or a description of when to log out
17. Establish and administer privileged user accounts in accordance with a role-based access scheme
18. Monitor all privileged role assignments
19. Take defined actions once users no longer require privileged role assignments
20. Require that organization defined conditions be met to permit the use of shared or group accounts
21. Terminate or change shared or group account credentials when members leave the group
22. Monitor system accounts for atypical usage
23. Report any detection of atypical usage on system accounts to defined personnel or roles

## Access Enforcement

Approved authorizations for logical access to the system will be enforced in accordance with applicable Organization Name defined, identity-based, role-based, attribute-based policies.

## Information Flow Enforcement

To regulate where information can travel, Organization Name information systems enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. Acceptable information flow is based on organization-defined information flow control policies.

Organization Name information systems separate the information flow logically or physically using defined mechanisms and/or techniques to accomplish defined separation by information type.

## Separation of Duties

Organization Name maintains a “separation of duties” framework that has been documented and implemented across the organization to define the duties of individual employees, prevent malicious activity without collusion, and assign information system access authorizations. The separation of duties framework can be found as System Security Plan (SSP) Attachment 11.

## Least Privilege

Organization Name follows the “least privilege” concept. Only the minimum necessary system preferences required to perform job duties are granted to an individual. The following measures have been put in place to ensure compliance with the least privilege requirements:

1. Explicit authorization must be granted thru the account authorization process to receive authorized access to a service provider defined list of security functions and relevant security information.
2. Individuals with access to information system accounts, roles, or other security functions are required to use a unique, non-privileged account when performing non-administrative functions.
3. Privileged accounts on the information system are restricted to predefined personnel or roles.
4. Information systems regularly audit the execution of privileged functions.
5. Non-privileged users are prevented from executing privileged functions including disabling, circumventing, or altering implemented security safeguards or countermeasures.

## Unsuccessful Log in Attempts

Users are limited to three (3) consecutive invalid log-in attempts during a fifteen (15) minute period. If the user exceeds the maximum number of unsuccessful log-in attempts, the account/node will be automatically locked for thirty (30) minutes.

## System Use Notifications

Organization Name information systems are configured to display a system use notification when users access the information system. Additionally, Organization Name information system retains the notification message or banner on the screen until explicit acknowledgement and action is taken to log on to or further access the information system.

The system use notification must include the following information:

1. Users are accessing a U.S. Government information system
2. System usage may be monitored, recorded, and subject to audit
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties
4. Use of the system indicates consent to the monitoring and recording

Publicly accessible Organization Name systems display the following information:

1. System use information when appropriate, before granting further access
2. References, if applicable, to monitoring, recording, or auditing, that are consistent with privacy accommodations for such systems that generally prohibit those activities
3. A description of authorized usage

## Concurrent Sessions

Organization Name limits the number of concurrent sessions for privileged users to three (3) sessions and two (2) sessions for non-privileged users.

## Session Lock and Termination

Organization Name information systems have a session lock that is triggered after no more than fifteen (15) minutes of inactivity or upon receiving a user request. The system will retain the session lock until the user re-established access using their Organization Name identification.

Upon activation of a session lockout, information previously visible on the display is concealed with a publicly viewable image. User sessions will be automatically terminated after 15 minutes.

## Permitted Actions without Identification or Authentication

User actions that can be performed on information systems without identification or authentication are documented in the System Security Plan (SSP).

## Remote Access

Usage restrictions, configuration and connection requirements, and implementation guidance have been established and documented for each type of remote access allowed by Organization Name. All remote access to the information system is authorized prior to allowing such connections.

Organization Name uses Insert SIEM/Log Aggregation Tool to facilitate the monitoring and control of remote access methods, allowing event auditing across information system components. The confidentiality and integrity of all remote access sessions is protected using encryption and the information system is configured to route all remote accesses through a limited number of managed access control points (e.g., external firewall, load balancer, etc.).

Execution of privileged commands and access to security-relevant information via remote access are only authorized for compelling operational needs, and the rationale for providing authorization is documented in the System Security Plan (SSP). Any unauthorized remote access connections to the system will be disconnected within fifteen (15) minutes of discovery.

## Wireless Access

To ensure secure wireless access and wireless operations, usage restrictions, configuration and connection requirements, and implementation guidance have been established for all wireless access.

All wireless access to information systems must be explicitly authorized prior to establishing connections and all wireless access to the system is protected using authentication and encryption, while ensuring authentication is applied to users, devices, or both as necessary.

## Access Control for Mobile Devices

Organization Name has implemented usage restrictions and implementation guidance for organization-controlled mobile devices. All mobile device connections, given they meet established usage restrictions, must be authorized and full-device encryption and/or container encryption will be implemented to protect the confidentiality and integrity of the information on defined mobile devices.

## Use of External Information Systems and Information Sharing

Where applicable, Organization Name has established terms and conditions allowing authorized access to Organization Name information systems from external information systems. Additional terms and conditions have been established allowing authorized individuals to process, store, and/or transmit Organization Name-controlled information using the external information systems.

Organization Name permits authorized individuals to use an external information system to access Organization Name systems or to process, store, or transmit organization-controlled information only when the implementation of required security can be verified on the external system, in accordance with the Organization Name information security policy and security plan.

Organization Name also permits the connections described in AC-20(1)(a) of the System Security Plan (SSP) if the user has an approved information system connection or processing agreement with the organizational entity hosting the external information system.

The use of Organization Name-controlled portable storage devices by authorized individuals on external information systems is prohibited.

To facilitate information sharing, Organization Name has enabled authorized users with the ability to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for defined information sharing circumstances where user discretion is required. Additionally, Organization Name must employ defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

## Publicly Accessible Content

Only designated and authorized individuals are permitted to post publicly accessible information onto the information system. Authorized individuals are trained to ensure that publicly accessible information does not contain non-public information.

All content will be reviewed for non-public information before it is posted onto Organization Name information system as publicly accessible. All information published as publicly will be reviewed for non-public information at least quarterly and any such information will be removed from the information system.