Insert Logo Here

Organization Name

Security Procedures

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 Procedures | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68597261)

[2 Purpose 1](#_Toc68597262)

[3 Scope 1](#_Toc68597263)

[4 Roles and Responsibilities 1](#_Toc68597264)

[5 Management Commitment 2](#_Toc68597265)

[6 Authority 3](#_Toc68597266)

[7 Compliance 3](#_Toc68597267)

[8 Procedural Requirements 4](#_Toc68597268)

[8.1 Access Control Policies and Procedures 4](#_Toc68597269)

[8.2 Account Management 4](#_Toc68597270)

[8.2.1 Account Identification 4](#_Toc68597271)

[8.2.2 Adding New Users 4](#_Toc68597272)

[8.2.3 Removing Terminated or Transferred Users 5](#_Toc68597273)

[8.2.4 Current Users 5](#_Toc68597274)

[8.2.5 Shared & Group Accounts 5](#_Toc68597275)

[8.3 Auditing of Privileged Accounts 5](#_Toc68597276)

[8.4 System and Account Parameters 5](#_Toc68597277)

[8.5 System Warning Banner 6](#_Toc68597278)

[8.6 Information Flow Enforcement 6](#_Toc68597279)

[8.7 Separation of Duties and Least Privilege 7](#_Toc68597280)

[8.8 Permitted Actions without Identification or Authentication 7](#_Toc68597281)

[8.9 Remote Access 8](#_Toc68597282)

[8.9.1 VPN Client 8](#_Toc68597283)

[8.9.2 Auditing and Monitoring 8](#_Toc68597284)

[8.10 Configuring Wireless Access 8](#_Toc68597285)

[8.11 Configuring Mobile Device Access 8](#_Toc68597286)

[8.12 External Information Systems and Information Sharing 9](#_Toc68597287)

[8.13 Publicly Accessible Information 9](#_Toc68597288)

[9 APPENDIX A: LIST OF USERS PERMITTED TO ACCESS THE DATACENTER 10](#_Toc68597289)

[10 APPENDIX B: LIST OF USERS WITH REMOTE ACCESS PRIVILEGES 10](#_Toc68597290)

[11 APPENDIX C: LIST OF USERS WITH PUBLICLY ACCESSIBLE CONTENT PRIVILEGES 10](#_Toc68597291)

[12 APPENDIX D: LIST OF CURRENT EXTERNAL INFORMATION SYSTEMS 11](#_Toc68597292)

# 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 system access control procedures. These procedures are in place to facilitate the implementation of the Access Control 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 procedures 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 procedure. 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 procedure 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 access control security 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

The Information Security Manager is responsible for developing, disseminating, reviewing, and updating these procedures on an annual basis in order to facilitate the implementation of the access control procedure and associated access controls.

## Account Management

Organization Name personnel shall establish, activate, modify, disable, and remove accounts in accordance with the procedures herein.

### Account Identification

The Information Security Manager must annually review the following types of information system accounts to support organizational missions/business functions:

* Account type

Service accounts are created and managed through the Change Management board and System administrators use Tool to support the management of system accounts in accordance with the procedures herein.

### Adding New Users

To add a new user to the information system, approval by the appropriate account manager {Roles} must be obtained. Once approval is granted, the new user can be added to the system.

New user accounts will be assigned in the following systems:

* Systems

The table below outlines the different account types and various access privileges defined by role.

|  |  |  |
| --- | --- | --- |
| Account Type | Role | Access Description |
|  | System Administrator | Has domain level privileges for full administrative access to servers in the security boundary. |
| Database Administrator | Has full administrative access to the databases inside the security boundary. |
| Information Security Administrator | Has local administrative permissions on the servers to security functions |
| SCCM Administrator | Has local administrative permissions on the servers to apply patches and deploy software installations. |
|  |  |

Account Managers are created for all account types. Only the individuals listed below are authorized to act as an Account Manager for the specified account type.

* Insert Accounts types and account managers

Once a new user account has been created, a notification will be sent to the user containing their log in credentials.

### Removing Terminated or Transferred Users

When a user account is deleted due to termination or transfer, all access privileges must also be removed. If a user is transferring and needs or does not need certain privileges, the {Role} must submit a ticket to request the specific privileges be add or removed to the user account.

Upon completion of user account changes, a notification will be sent to the user and reporting manager stating that the user’s privileges have been updated.

In the event of privilege removal, the {Role} use {Tool} to update the user’s privileges. This action is performed once a user completes an assigned task or during the account compliance check performed annually or during an access control reviews conducted quarterly for privileged account types.

### Current Users

The {Roles} review all accounts on a quarterly basis. Organization Name has implemented domain policies in {Tool}, to ensure the information system is configured to disable inactive user accounts after ninety (90) days.

### Shared & Group Accounts

Organization Name does/does not allow shared and/or group accounts to be created in the information system.

## Auditing of Privileged Accounts

Event auditing through event logs on the accounts are in use and applied to the creation of new accounts, a change in access, disabling, or termination actions. {Role} reviews {Tool} dashboards weekly for these event types.

For any account changes, {Role} will verify that either a ticket regarding user permissions or a Change Management request regarding a service account is associated with the event.

If a ticket or a Change Management request does not exist, the {Role} will disable the account and begin an investigation in coordination with the {Role} regarding the account’s creation. Corrective actions and/or activation of the incident response process are relevant outcomes as well as remediation training on process if deemed appropriate.

All privileged role assignments are monitored and recorded by {Tool} Privileged user accounts are monitored for unusual behavior including accessing accounts from locations that are not considered normal using {Tool}.

## System and Account Parameters

has implemented the following system and account security requirements and parameters:

* {Tool} are configured to enforce lockout limits to be set to three (3) invalid login attempts within a fifteen (15) minute time period.
* Mechanisms are employed to automatically lock a user session after fifteen (15) minutes of inactivity and systems shall retain the session lock until the user reestablishes access using authenticated means of reconnection with valid username and password.
* Upon session lock, assets shall be configured to conceal information system information previously visible on the display with a publicly viewable image.
* In accordance with CIS Level 1 requirements, accounts will auto-unlock fifteen (15) minutes after an account lockout occurs.
* In accordance with the Organization Name Rules of Behavior and Acceptable Use Policy, all users are required to execute the keyboard function CTL+ALT+DEL and lock their computer when they expect to be away from their workstation.
  + Violation of this policy is subject to disciplinary actions in accordance with the Organization Name Rules of Behavior and Acceptable Use Policy.
* Under the domain policy, accounts are configured to limit concurrent sessions. Each account or account type should be limited to certain number of concurrent sessions, non-privileged accounts are limited to three sessions, privileged accounts are limited to two (2) sessions.
  + Back-end/Management sessions: Limited via {Operating System} constraints via {Remote Access Tool} to jump servers to one privileged session. Non-privileged accounts do not exist for back-end management.
  + Web sessions: Limited to two sessions for all account types.

## System Warning Banner

Organization Name enforces the user of a system “warning” banner which displays privacy and security notices including the statements listed below. The banner will remain displayed on the screen until users manually select the “Accept” or “OK” button to proceed with the log in process.

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

For the publicly accessible web application, system use information and warning banner is displayed beneath the statement “By logging in an above, you agree to the below statement.” Consent with the system use requirements is granted when the user logs in to the system.

## Information Flow Enforcement

The {Role} determines information flow implementation. Information flow is controlled, and approved authorizations are enforced by:

* Filtering and routing policies on {Network Security Functions}
* Through the use of {Tool} security groups delegated, write, execute, etc. permissions assigned to roles, folders, and/or files and databases through access control lists.
* Access control to the information system is enforced through security groups, roles, unique User IDs and passwords, multi-factor authentication, and access rights based on the least privilege principle.
* The system separates information flow logically using segmented subnets with {Network Security Functions} that limit traffic to provide {Level of separation} of customer tenants and data.

## Separation of Duties and Least Privilege

Organization Name enforces separation of duties and the “least privilege” principle by ensuring that various roles are assigned to different personnel and personnel are not assigned responsibilities intended for other job functions. Least privilege means that an individual only has access to the systems and tools they need to perform their job.

Roles such as {List Roles} are carried out by separate individuals.

Typical user accounts do not have permissions to {List Limitations} For complete permissions details, see the *Separation of Duties Matrix*.

The following separation of duties policies are to be maintained at all times:

* Information system access authorizations must be documented to support the separation of duties and individual duties will be managed through the *Access Control Policy*, role membership, and permission settings
* Roles and groups within the system govern what users are able to see and do through global security group memberships, specific database permissions, and application roles. Features and functions of the system are only available to select users based on job function.
* Duties are explicitly assigned as needed to meet organizational objectives, ensuring the separation of duties is documented.
* Privileged accounts are restricted to {Roles} staff in order to limit access and securely operate the information system.
* The assignment of responsibilities required to support the network, applications, and systems are split into multiple {Tool} Administrative Security roles defined in the *Separation of Duties Matrix*.
* Individuals do not have access permissions to devices, systems, and applications outside of their support responsibilities.
* Application and operating system event logging and automated logging mechanisms are used to audit and monitor the execution of privileged accounts.

## Permitted Actions without Identification or Authentication

All actions permitted within the web application and back-end access require identification and authentication to access the appropriate system. There are {no/#} publicly accessible systems or web facing applications that can be accessed or actions taken without proper identification and authorization.

## Remote Access

### VPN Client

Organization Name has implemented and enforces the following requirements for the implementation and use of the VPN Client:

* The {Role} must first sign off on any remote access privileges for system {Tool} Access prior to their allocation.
* An ticket including supporting rationale for submitting the request must be submitted before VPN access is granted.
* New users are only granted VPN access after an ticket has been submitted and approved.
  + The user’s credentials are generated via {Explain}
* The VPN client enforces a two-factor authentication credential that utilizes modern encryption.
  + The current authentication credentials include {MFA Used} as well as username and password.
* The VPN client enforces a Modern encryption, multi factor encryption and routes all remote access traffic through redundant firewalls.
* The VPN will time out after fifteen (15) minutes of inactivity.
* The VPN will force all users to re-authenticate after eight (8) hours.
* {Tool} maintains the list of VPN users assigned to the {Group Name}.

### Auditing and Monitoring

For VPN users with remote access, including those users with {Tool} Administrative privileges, Organization Name has configured the VPN infrastructure to generate audit logs for each remote access connection, disconnection, and session.

Organization Name has implemented a deny all, permit by exception rule for incoming traffic for Ports, protocols, and services. Allowed Ports, protocols, and services are listed in the SSP and rules are configured in {Firewall Tool}

In the event an unauthorized remote connection is detected, {Role} will connect to the {System} and {Explain how remote connection will be terminated}

## Configuring Wireless Access

This is an inherited control. See {List IaaS/PaaS SSP info}.

## Configuring Mobile Device Access

This is an inherited control. See {List IaaS/PaaS SSP info}.

## External Information Systems and Information Sharing

Organization Name {does/does not} allow external systems to access the information system. If external systems need access to the information system, the following will apply:

* The external system must be StateRAMP Authorized at and equal category level.
* An appropriate interconnection security agreement is provided and approved by the Authorizing Official.

A formal and documented access request has been submitted and terms and conditions setting the scope of the access have been agreed upon and approved by the {Role} prior to access being granted to the external system.

* The {Role} shall retain connection or processing agreements with the external entity and validate that the external information systems have the following security controls in place:
  + The latest operating system security patches
  + Current antivirus software running in the background
  + Support of approved encryption for connection to the information system
  + A means of auditing and alerting
* Any findings regarding the external information system’s security controls will be documented and retained.

When dealing with information sharing, Organization Name will have authorized users who are able to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for incident response, risk assessments, emergency maintenance, and/or third-party audits.

To assist users in making information sharing and collaboration decisions, Organization Name shall employ access control, information flow monitoring (in accordance with the *System and Communications Protection Policy* and procedures), and media restrictions (in accordance with *Media Protection Policy* and procedures).

## Publicly Accessible Information

There {is/is not} publicly accessible information on the information system. Individuals who post information on to publicly accessible information systems are designated and have been properly authorized. Prior to posting information on a publicly accessible system, the contents of the post must be reviewed for non-public information. As part of ongoing security awareness, the {Role} is responsible for training those individuals or groups responsible for reviewing all publicly accessible content.

The following actions are taken during the quarterly review for non-public information:

* Review of all publicly information systems and ensure no non-public information has been published
* Documentation of all findings.
* Any sensitive content that is publicly accessible will be immediately removed and the Information Security Team will be notified

# APPENDIX A: LIST OF USERS PERMITTED TO ACCESS THE DATACENTER

In accordance with this policy, the following individuals (including employees, contractors, or vendors) are permitted to access the information datacenter locations without an escort:

|  |  |
| --- | --- |
| **Name** | **Data Center Location** |
|  |  |
|  |  |

# APPENDIX B: LIST OF USERS WITH REMOTE ACCESS PRIVILEGES

In accordance with this policy, the following individuals (including employees, contractors, or vendors) are permitted to remotely access the information system:

|  |  |  |
| --- | --- | --- |
| **Name** | **Title/Job Role** | **Type of Method/Encryption** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# APPENDIX C: LIST OF USERS WITH PUBLICLY ACCESSIBLE CONTENT PRIVILEGES

In accordance with this policy, the following individuals (including employees, contractors, or vendors) are permitted to post and manage the publicly accessible content of the information system:

|  |  |
| --- | --- |
| **Name** | **Title/Job Role** |
|  |  |

# APPENDIX D: LIST OF CURRENT EXTERNAL INFORMATION SYSTEMS

In accordance with this policy, the following external information systems have been approved by the information Executive Management team for the information system:

|  |  |
| --- | --- |
| **Name** | **Purpose** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |