Insert Logo Here

Organization Name

Security Procedure

Audit & Accountability

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 AU Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68598968)

[2 Purpose 1](#_Toc68598969)

[3 Scope 1](#_Toc68598970)

[4 Roles and Responsibilities 1](#_Toc68598971)

[5 Management Commitment 2](#_Toc68598972)

[6 Authority 3](#_Toc68598973)

[7 Compliance 3](#_Toc68598974)

[8 Procedural Requirements 4](#_Toc68598975)

[8.1 Configuring Auditable Events 4](#_Toc68598976)

[8.2 Auditable Events 4](#_Toc68598977)

[8.3 Configuring Audit Records 5](#_Toc68598978)

[8.4 Configuring Audit Storage Capacity & Alerts 5](#_Toc68598979)

[8.5 Reviewing Audit Records 5](#_Toc68598980)

[8.6 Information System Configuration 6](#_Toc68598981)

[8.6.1 Initial Date/Time Configuration 6](#_Toc68598982)

[8.6.2 Synchronizing Date/Time Information 6](#_Toc68598983)

[8.7 Protecting Audit Logs and Audit Log Retention 6](#_Toc68598984)

[8.7.1 Audit Log Protection 6](#_Toc68598985)

[8.7.2 Audit Log Retention 7](#_Toc68598986)

# 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 Audit & Accountability 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 audit and accountability procedures. These procedures are in place to facilitate the implementation of the Audit and Accountability Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# Scope

The provisions of these policies pertain to all Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for Organization Name information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization Name and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization Name Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these procedures is mandatory. It is Organization Name policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Procedural Requirements

The following audit and accountability 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.

## Configuring Auditable Events

The information system implements audit logging mechanisms for the information system and application using the audit logging solution, {Tool}.

{Tool}is capable and will be configured to provide audit reduction and generate dashboards, including audit records that are based on selectable event criteria. {Tool} is the location where the data displayed through {Tool} retained. {Tool} can be used to produce on-demand reports. {Tool} supports on-demand review and analysis of events. {Tool} supports reporting and after-the-fact investigation of security incidents. {Tool} is also configured to not alter the original content or time ordering of audit records. If a new audit logging solution is being considered, the {Role} shall verify that the solution is capable of audit reduction and report generation.

## Auditable Events

Auditable events are to be defined for the information system and web application where applicable. It is the responsibility of the {Role} to define the list of auditable events within the settings of the audit logging solution.

Security audit functions will be coordinated with other Organization Name entities such as {Roles/Teams} requiring audit-related information. Using {Tool}, the {Roles/Teams} will configure the following minimum auditable events:

* **Information System:** {Tool}
	+ Successful and unsuccessful account logon events
	+ Account management events (e.g. new account created, user account deleted, etc.)
	+ Policy changes
	+ Privilege functions (e.g. administrator activity)
	+ System events or syslogs
* **Web Application:** {Tool}
	+ Administrator activity
	+ Authentication checks
	+ Authorization checks
	+ Sensitive data deletions
	+ Sensitive data access
	+ Sensitive data changes
	+ Permission changes
* **{Security Tools}:** {Tool}
	+ Threat events
	+ Application control events
	+ Host Intrusion Prevention System (HIPS) events
	+ Firewall deny events
* **{Network Tools}:** {Tool}
	+ All inbound and outbound network logs
* **{VPN}:** {Tool}

It is the responsibility of the {Role} to review and update the list of each auditable event on an annual basis or change in the threat environment through the change security risk assessment.

## Configuring Audit Records

When applicable, the information system and web application are configured to produce audit records. At a minimum, {Tool} is configured to produce the following content:

* Type of event
* Data and time of the event
* Source of the event
* Outcome of the event (either success or failure)
* Identity of the user/subject associated with the event

The audit logging solution on the information system within the Network flow logs will be configured to log the following:

* Session, connection, transaction, or activity duration
* For client-server transactions: the number of bytes received and sent
* Additional informational messages to diagnose or identify the event
* Characteristics that describe or identify the object or resource being acted upon

The {Role} will validate periodically that the audit records contain the above audit record content.

## Configuring Audit Storage Capacity & Alerts

{Tool} is configured with appropriate audit storage capacity. {Tool} has a 365 day retention policy and automatically scales storage for the retention timeline requirement.

If an audit log processing failure occurs, the following actions shall be taken:

* The {Roles/Teams} are automatically alerted that failure has occurred via {Alerting Medium} on {Tool}
* The information system retains 365 days of auditing and the solution will automatically scale to meet the storage requirements

## Reviewing Audit Records

The {Role} will review and analyze all audit information system audit records within {Tool} on a weekly basis. If unusual or inappropriate findings are detected, the findings shall be reported to the {Role} immediately.

For internal security incidents, the Organization Name {Role} shall open an incident record. Such findings should be documented and tracked using the procedure outlined in the Incident Response Plan.

Additionally, the {Role} will adjust the level of audit review, analysis, and reporting within the information system if there is a change in risk to the environment. The {Roles/Teams} work together to meet the auditing requirements if an adjustment needs to be made.

Organization Name shall employ {Tool} and the ticketing system to integrate audit review, analysis, and reporting processes to support processes for investigation and response to suspicious activities.

Organization Name will leverage {Tool} to gain information wide situational awareness through the analysis and correlation of audit records.

## Information System Configuration

### Initial Date/Time Configuration

{Tool} is configured with appropriate time stamps using the following steps:

1. {Tool} in the environment receive their time from the NIST authoritative time source.
2. All Servers in the environment sync their system clocks with the domain controller.
3. {Tool} receive their time from the client systems forwarding events.

### Synchronizing Date/Time Information

For time synchronization, configure the information system and system components to synchronize with the NIST time server every 6-10 minutes or when skew is greater than three (3) minutes.

As a rule, the information system uses the NIST authoritative time source as the primary time server. NIST time servers are load balanced and geographic redundancy is built into the NIST time service.

## Protecting Audit Logs and Audit Log Retention

### Audit Log Protection

Audit logs stored within {Tool} will be replicated from the primary site {Primary Data Center} to the alternate site {Secondary Data Center}. Audit logs and tools will be protected from any unauthorized access, modification, or deletion through role-based access control (RBAC). Only approved and authorized users are to be permitted access to the audit logs within {Tool}. The current list of administrators includes {Role/Team}. To add a new administrator or user to the audit logging solution(s), the following steps are to be taken:

* Validate that a document request has been generated through the {Ticketing Solution}.
* Set the appropriate privileges within the audit logging solution.

As part of the quarterly access review process, validate that the list of admins and users is current and only necessary privileges are applied.

### Audit Log Retention

{Tool} is configured to store audit logs for ninety (90) days online for immediate review and analysis and three hundred and sixty five (365) days offline/storage.