

{Insert Company Name}

Security Policy

Audit and Accountability

**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

[Document Revision History 0](#_Toc189232232)

[Table of Contents 1](#_Toc189232233)

[1 Introduction 0](#_Toc189232234)

[2 Purpose 0](#_Toc189232235)

[3 Scope 0](#_Toc189232236)

[4 Roles and Responsibilities 0](#_Toc189232237)

[5 Management Commitment 1](#_Toc189232238)

[6 Authority 2](#_Toc189232239)

[7 Compliance 2](#_Toc189232240)

[8 Policy Requirements 0](#_Toc189232241)

[8.1 Audit and Accountability Policies and Procedures [AU-1] 0](#_Toc189232242)

[8.2 Event Logging [AU-2] 0](#_Toc189232243)

[8.3 Content of Audit Records [AU-3, AU-3 (1)] 1](#_Toc189232244)

[8.4 Audit Storage Capacity [AU-4] 1](#_Toc189232245)

[8.5 Response to Audit Processing Failures [AU-5, {AU-5 (1,2) High Only}] 2](#_Toc189232246)

[8.6 Audit Record Review, analysis, and Reporting [AU-6, AU-6 (1,3), {AU-6 (4,5,6,7) High Only}] 2](#_Toc189232247)

[8.7 Audit Record Reduction and Report Generation [AU-7, AU-7 (1)] 3](#_Toc189232248)

[8.8 Time Stamp[AU-8] 3](#_Toc189232249)

[8.9 Protection of Audit Information [AU-9, AU-9 (4), {AU-9 (2,3) HIGH ONLY}] 3](#_Toc189232250)

[8.10 Non-Repudiation [{AU-10 High Only}] 4](#_Toc189232251)

[8.11 Audit Record Retention [AU-11] 4](#_Toc189232252)

[8.12 Audit Generation [AU-12, {AU-12 (1,3) High Only}] 4](#_Toc189232253)

# 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 Audit and Accountability Policies and Procedures [AU-1]

This document is intended to serve as the *Audit and Accountability Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Audit and Accountability 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: [AU-1 (a)]

* An organizational-level Audit and Accountability Policy that: [AU-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [AU-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [AU-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Audit and Accountability Policy and the associated Audit and Accountability controls [AU-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Audit and Accountability policy and procedures. [AU-1 (b)]

{Insert Company Name} must review and update the current Audit and Accountability: [AU-1 (c)]

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

8.2 Event Logging [AU-2]

As {Insert Company Name} must coordinate the event logging function with other organizational entities requiring audit related information to enhance support and to guide the selection of auditable events. [AU-2 (b)]

{Insert Company Name} must identify the types of events that the system is capable of logging and determined the type of events required to be logged to support after-the-fact investigations of security incidents. [AU-2 (a, d)]

{Insert Company Name} shall, at a minimum, collect all the following events from event sources from each {Insert Company Name} information system. [AU-2 (c)]

* {Insert Company Name} must ensure that infrastructure continually logs the following events:
  + Successful and unsuccessful account logon events
  + Account management events
  + Object access
  + Policy change
  + Privilege functions
  + Process tracking
  + System events
* {Insert Company Name} must ensure that web applications are continually logging the following events:
  + Administrator activity
  + Authentication checks
  + Authorization checks
  + Data deletions
  + Data access
  + Data changes
  + Permission changes

{Insert Company Name} must ensure that additional events can be logged, as needed, to support troubleshooting of issues such as infrastructure, web application issues, or security incidents. [AU-2 (c)] {Insert Company Name} should review and update the logged events annually or whenever there is a change in the threat environment. [AU-2 (e)] Capabilities must be in place to log additional events based on current threat information and ongoing risk assessment.

8.3 Content of Audit Records [AU-3, AU-3 (1)]

{Insert Company Name} must ensure that the information system generates audit records that contain, at a minimum, the following information:

1. Type of event [AU-3 (a)]
2. Date and time of the event [AU-3 (b)]
3. Location of the event [AU-3 (c)]
4. Source of the event [AU-3 (d)]
5. Outcome of the event (success or failure) [AU-3 (e)]
6. Identity of the individuals, subjects, or objects/entities associated with the event [AU-3 (f)]

Audit records must be generated containing the following additional information when available: [AU-3 (1)]

* Session, connection, transaction, and/or activity duration
* The number of bytes received and bytes sent for client-server transactions
* Additional informational messages to diagnose or identify the event
* Characteristics that describe or identify the object or resource being acted upon
* Individual identities of group account users
* Full text of privileged commands

8.4 Audit Storage Capacity [AU-4]

{Insert Company Name} must allocate audit record storage capacity and configure audit logging to reduce the likelihood of capacity being exceeded. [AU-4] This may include using auto-provisioning technologies to dynamically allocate more storage, when needed.

8.5 Response to Audit Processing Failures [AU-5, {AU-5 (1,2) High Only}]

{Insert Company Name} shall ensure that the system alerts the {Insert Company Name} Technology Team in near real-time in the event of an audit logging processing failure [AU-5 (a)] and overwrites the oldest record until the failure is remediated [AU-5 (b)].

**For high impact systems only:**

{Insert Company Name} shall ensure a warning is provided to designated IT/IS personnel within four (4) hours when allocated audit log storage volume reaches seventy-five (75) percent of repository or one month before maximum audit log storage is expected to be negatively impacted. [AU-5 (1)] {Insert Company Name} also ensures an alert is provided in near real-time to IT/IS personnel with authority to address failed audit events, when audit events requiring real-time alerts fail. [AU-5 (2)]

8.6 Audit Record Review, analysis, and Reporting [AU-6, AU-6 (1,3), {AU-6 (4,5,6,7) High Only}]

{Insert Company Name} must review and analyze information system audit records at least weekly. At a minimum, this review should include analysis for indications of inappropriate or unusual activity as it relates to account usage, privileged access requests, data access requests, and suspicious SQL queries. [AU-6 (a)]

Audit findings must be reported to the Information Security Team [AU-6 (b)] so adjustments can be made to the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information or other credible sources of information to organizational operations, assets, and individuals. [AU-6 (c)]

{Insert Company Name} must employ automated event alert reporting to integrate audit review, analysis, and reporting processes. [AU-6 (1)] Automated event alert reporting supports organizational processes for incident response, continuous monitoring, and investigation and response to suspicious activities. {Insert Company Name} must analyze and correlate audit records across different repositories to gain organization-wide situational awareness. [AU-6 (3)]

**For high impact systems only**

{Insert Company Name} must:

* Provide and implement the capability to centrally review and analyze audit records from multiple components within the system [AU-6 (4)]
* Integrate analysis of audit records with analysis of vulnerability scanning information, performance data, and system monitoring information from SIEM data and information collected from other sources to further enhance the ability to identify inappropriate or unusual activity [AU-6 (5)]
* Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity [AU-6 (6)]
* Specify the permitted actions for each information system process, role, or user associated with the review, analysis, and reporting of audit record information [AU-6 (7)]

8.7 Audit Record Reduction and Report Generation [AU-7, AU-7 (1)]

{Insert Company Name} must provide and implement an audit record reduction and report generation capability that:

* Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of security incidents [AU-7 (a)]
* Does not alter the original content or time ordering of audit records [AU-7 (b)]

Additionally, {Insert Company Name} must provide and implement the capability to process, sort, and search audit records for events of interest based on fields within event records including: [AU-7 (1)]

* Type of event
* Date and time of the event
* Location of the event/IP addresses involved
* Source of the event
* Outcome of the event (success or failure)
* Identity of the individuals, subjects, or objects/entities /subject associated with the event

8.8 Time Stamp[AU-8]

{Insert Company Name} must ensure that information systems:

* Use internal system clocks to generate time stamps for audit records [AU-8 (a)]
* Record time stamps for audit records within one second of granularity and meets at least one of the following criteria: [AU-8 (b)]
  + Uses Coordinated Universal Time (UTC),
  + Has a fixed local time offset from UTC, or
  + Includes the local time offset as part of the time stamp

8.9 Protection of Audit Information [AU-9, AU-9 (4), {AU-9 (2,3) HIGH ONLY}]

{Insert Company Name} must protect audit information and logging tools from unauthorized access, modification, and deletion. [AU-9 (a)] The Information Security Team must be alerted upon detection of unauthorized access, modification, or deletion of audit information. [AU-9 (b)]

Access to the management of audit logging functionality must be limited to only privileged roles requiring access and must be properly authorized by both the Information Security manager and Information Technology manager. [AU-9 (4)].

**For high impact systems only**

{Insert Company Name} must:

* Backup or store audit records at least weekly in a repository that is part of a physically different system or system component from the system or component being audited [AU-9 (2)]
* Implement cryptographic mechanisms to protect the integrity of audit information and audit tools (see AC-13) [AU-9 (3)]

8.10 Non-Repudiation [{AU-10 High Only}]

**For high impact system only:**

{Insert Company Name} must provide irrefutable evidence that an individual or process acting on behalf of the individual has performed actions including the addition, modification, deletion, approval, sending, or receiving of data. [AU-10]

8.11 Audit Record Retention [AU-11]

{Insert Company Name} shall retain audit records online for at least ninety (90) days. For systems hosting Federal data, {Insert Company Name} must further preserve audit records offline for a period in accordance with NARA and M-21-31 and/or client requirements to support after-the-fact investigations of security and to meet regulatory and organizational retention requirements. [AU-11]

8.12 Audit Generation [AU-12, {AU-12 (1,3) High Only}]

{Insert Company Name} must ensure that information systems:

* Provides an audit record generation capability for the list of auditable events defined in section 8.2 (AU-2) above on all information system and network components where audit capability is deployed/available [AU-12 (a)]
* Allows Information Security and Information Technology Management to select which events are to be audited by specific components of the system [AU-12 (b)]
* Generates audit records for the list of audited events defined in Section 8.2 above (AU-2c) with the content as defined in Section 8.3 above (AU-3) [AU-12 (c)]

**For high impact systems only:**

{Insert Company Name} must:

* Compile audit records from all network, data storage, and computing devices into a system-wide logical audit trail that is time-correlated within one (1) second of granularity to time stamps of individual records in the audit trail [AU-12 (1)]
* Provide and implement the capability for roles with audit configurations responsibilities to change the logging to be performed on all network, data storage, and computing devices based on event types to facilitate audit reduction, analysis, and reporting. {Insert Company Name} requires logging actions to be able to be changed within one (1) hour of the approved scheduled time. [AU-12 (3)]