

{Insert CompanY Name}

Security Procedures

Audit and Accountability [AU]

**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 Procedural Requirements [AU-1] ............................................................................................................. 4

8.2 Event Logging [AU-2] ........................................................................................................................ 4

8.3 Configuring Audit Records [AU-3] .................................................................................................... 5

8.4 Configuring Audit Storage Capacity & Audit Processing Failure [AU-4, AU-5] ................................. 6

8.5 Reviewing Audit Records [AU-6] ...................................................................................................... 6

8.6 Audit Record Reduction and Report Generation [AU-7] .................................................................. 7

8.7 Information System Time Stamp Configuration [AU-8] ................................................................... 7

8.7.1 Initial Date/Time Configuration .................................................................................................. 7

8.7.2 Synchronizing Date/Time Information ....................................................................................... 7

8.8 Protecting Audit Logs and Audit Log Retention [AU-9, AU-11] ........................................................ 8

8.8.1 Audit Log Protection ................................................................................................................... 8

8.8.2 Audit Log Retention .................................................................................................................... 8

8.9 Audit Generation [AU-12] ................................................................................................................ 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}’ 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}’ 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}’ 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}’ 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.

# Procedural Requirements[AU-1]

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 {Insert Company Name} information systems.



## Configuring Auditable Events

The {Insert Product Name} Information System implements audit logging mechanisms for the information system and application using the audit logging solution, {Insert Security Information and Event Management (SIEM) tool name}.

{Insert Security Information and Event Management (SIEM) tool name} is capable and is configured to provide audit reduction and generate dashboards, including audit records that are based on selectable event criteria. {Insert Security Information and Event Management (SIEM) tool name} is the location where the data displayed through {Insert Security Information and Event Management (SIEM) tool name} is retained. {Insert Security Information and Event Management (SIEM) tool name} can be used to produce on-demand reports. {Insert Security Information and Event Management (SIEM) tool name} supports on-demand review and analysis of events. {Insert Security Information and Event Management (SIEM) tool name} supports reporting and after-the-fact investigation of security incidents. If a new audit logging solution is being considered, the {Insert Information Security Team Name} shall verify that the solution is capable of audit reduction and report generation.

* 1. **Event Logging [AU-2]**

Auditable events are defined for the {Insert Product Name} Information System where applicable. The {Insert Information Security Team Name} coordinates the security audit function with the {Insert Information Technology Team Name} and {Insert Development Team Name} Teams to enhance mutual support and to help guide the selection of auditable events. [AU-2 (b)] If it is determined that changes to the current implementation of the auditable events is required, the {Insert Information Security Team Name} Manager works with the {Insert Information Security Team Name} and the {Insert Information Technology Team Name} to make changes to the identified logs.

Events are important for providing the ability to practice real-time monitoring of the information system, and for after-the-fact investigations of potential incidents. [AU-2 (d)] The {Insert Information Security Team Name} has configured {Insert Security Information and Event Management (SIEM) tool name} to continuously collect the following minimum auditable events: [AU-2 (a)]

* **{Insert Product Name} Information System:**

{Update list below as necessary}

* + {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}
* **{Insert Product Name} Application:** 
  + {Administrator activity}
  + {Authentication checks}
  + {Authorization checks}
  + {Sensitive data deletions}
  + {Sensitive data access}
  + {Sensitive data changes}
  + {Permission changes}
* **{Insert Antivirus Software Name} Client Logs:**

{Update list below as necessary}

* + {Threat events}
  + {Application Control events}
  + {Threat Prevention events}
  + {Firewall deny events}
* **{Insert Web Application Firewall tool name} (WAF):**

{Update list below as necessary}

* + {Blocked traffic}
  + {Anomaly scored traffic}
  + {Firewall rule violations}
* **{Insert name of hosting provider Portal} Logs:**

{Update list below as necessary}

* + All resource portal activity
* **Network Firewall Device Logs:**

{Update list below as necessary}

* + All inbound and outbound netflow logs
* **{Insert Identity Provider product name} Logs:**

{Update list below as necessary}

* + User session events

These events are continuously collected. [AU-2 (c)] The {Insert Information Security Team Name} and {Insert Information Technology Team Name} Teams review and update audited events at least annually or whenever there is a change in the threat environment. [AU-2 (e)] The teams review event types and, if changes need to be made, the auditable events are added, removed, or reconfigured in {Insert Security Information and Event Management (SIEM) tool name}.

* 1. **Configuring Audit Records [AU-3]**

When applicable, the {Insert Product Name} Information System is configured to produce audit records. At a minimum, {Insert Security Information and Event Management (SIEM) tool name} is configured to collect the following audit record contents:

* Type of event [AU-3 (a)]
* Data and time of the event [AU-3 (b)]
* Location of the event [AU-3 (c)]
* Source of the event [AU-3 (d)]
* Outcome of the event (either success or failure) [AU-3 (e)]
* Identity of the user/subject associated with the event [AU-3 (f)]

The audit logging solution on the information system within the network flow logs will be configured to log the following: [AU-3 (1)]

* 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
* Full text of privileged commands

The {Insert Information Security Team Name} will validate periodically that the audit records contain the above audit record content.

* 1. **Configuring Audit Storage Capacity & Audit Processing Failure [AU-4, AU-5]**

{Insert Company Name} utilizes {Insert Security Information and Event Management (SIEM) tool name} with at least a 365-day retention policy. [AU-4] {Insert Security Information and Event Management (SIEM) tool name} Workspace automatically scales storage to retain logs for at least 365 days in an online capacity and may remove the logs that have exceeded the 365-day retention rule. [AU-5 (b)]

If an audit log processing failure occurs, the {Insert Information Technology Team Name} and the {Insert Information Security Team Name} are automatically alerted that failure has occurred via {Insert Hosting Provider name} Health Alerts on {Insert Security Information and Event Management (SIEM) tool name}. [AU-5 (a)]

* 1. **Reviewing Audit Records [AU-6]**

The {Insert Information Security Team Name} reviews and analyzes all audit {Insert Product Name} Information System audit records within {Insert Security Information and Event Management (SIEM) tool name} on a weekly basis. During the weekly review, the Security Analyst looks for inappropriate or unusual activity as it relates to account usage, privileged access requests, data access requests, password resets, outgoing network traffic, application control events, antivirus threat events, and Web Application Firewall (WAF) blocked events. [AU-6 (a)] If a finding requires further investigation, it is reported to the {Insert Information Security Team Name}. [AU-6 (b)] The team analyzes the event to determine if it is an actual security incident or false positive. If the security event is flagged as an incident, the {Insert Information Security Team Name} Manager activates the Incident Response Plan (IRP). {Insert Company Name} notifies all customers based on the agreed upon times in each individual customer contract. For internal security incidents, the {Insert Company Name} Information Security Manager shall open a {Insert Company Name} security incident record. For {Insert Hosting Provider Name} managed findings, {Insert Hosting Provider Name} will notify the {Insert Company Name} {Insert Information Security Team Name}. Such findings should be documented and tracked using the procedure outlined in the IRP.

Additionally, the {Insert Information Security Team Name} will adjust the level of audit review, analysis, and reporting within the information system if there is a change in risk to the environment. [AU-6 (c)] The {Insert Information Security Team Name} and the {Insert Information Technology Team Name} work together to meet the auditing requirements if an adjustment needs to be made.

{Insert Company Name} uses {Insert Security Information and Event Management (SIEM) tool name} to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. [AU-6 (1)] {Insert Security Information and Event Management (SIEM) tool name} agents installed on Virtual Machines within the security boundary automatically collect events and forward them to the {Insert Security Information and Event Management (SIEM) tool name} workspace. {Insert Security Information and Event Management (SIEM) tool name} allows the {Insert Information Security Team Name} to apply rules and queries to conduct audit review analysis and create custom reports and alerts based on potential suspicious activities. {Insert Company Name} leverages {Insert Security Information and Event Management (SIEM) tool name} and {Insert Security Information and Event Management (SIEM) tool name} to gain information wide situational awareness through the analysis and correlation of audit records. Organizational situational awareness is represented across a commercial and government customer basis to improve security awareness. [AU-6 (3)]

* 1. **Audit Record Reduction and Report Generation [AU-7]**

{Insert Company Name} uses {Insert Security Information and Event Management (SIEM) tool name} to support on-demand audit review, analysis, and reporting requirements for the {Insert Product Name} Information System and other after-the-fact investigations of {Insert Product Name} security incidents. [AU-7 (a)] {Insert Security Information and Event Management (SIEM) tool name} correlates events from {Insert Product Name} system components, generates alerts, and report dashboards created by the {Insert Information Security Team Name}. The {Insert Information Security Team Name} use these alerts, dashboards, and reports to monitor the {Insert Product Name} Information System and investigate potential and confirmed security incidents. The {Insert Information Security Team Name} has configured the {Insert Security Information and Event Management (SIEM) tool name} dashboards to reduce the amount of information viewed by excluding insignificant events through event filtering queries.

{Insert Company Name} uses {Insert Name of SIEM query language} within {Insert Security Information and Event Management (SIEM) tool name} and {Insert Security Information and Event Management (SIEM) tool name} 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

{Insert Security Information and Event Management (SIEM) tool name} does not alter the original content of the audit records or timestamps of audit records generated by the {Insert Product Name} Information System. [AU-7 (b)] Logs are maintained in the {Insert Security Information and Event Management (SIEM) tool name} workspaces and protected via role-based access control.

* 1. **Information System Time Stamp Configuration [AU-8]**



### Initial Date/Time Configuration

{Insert Security Information and Event Management (SIEM) tool name} and {Insert Security Information and Event Management (SIEM) tool name} are configured with appropriate time stamps using the following steps:

1. {Insert Name of network NTP source} synchronize their time from the NIST authoritative time source using the list found at <https://tf.nist.gov/tf-cgi/servers.cgi>
2. {As a feature of Windows Active Directory, all member servers in the environment sync their system clocks with their domain controllers}
3. The {Insert Product Name} Information System utilizes the local server time for all logged events.
4. Events stored and reviewed with {Insert Security Information and Event Management (SIEM) tool name} have time stamps that can be mapped to Coordinated Universal Time (UTC). [AU-8 (a)]

### Synchronizing Date/Time Information

{Remove this section, if the product does not run on Windows}

The Windows Domain Controllers are configured to synchronize their clock times with the NIST authoritative time sources, documented at <http://tf.nist.gov/tf-cgi/servers.cgi>, at least hourly; all other servers in the environment sync their time from the domain controllers. If the clock is off by more than one second, it forces a resync immediately. NIST time servers load balance automatically, therefore geographic requirements for setting a secondary time server is not needed. [AU-8 (b)]

* 1. **Protecting Audit Logs and Audit Log Retention [AU-9, AU-11]**

### Audit Log Protection

Audit logs and tools will be protected from any unauthorized access, modification, or deletion through role-based access control (RBAC). [AU-9 (a)] Only approved and authorized users are to be permitted access to the audit logs within {Insert Security Information and Event Management (SIEM) tool name}. Alerts are configured using {Insert Security Information and Event Management (SIEM) tool name} to alert the {Insert Information Security Team Name} of detection of unauthorized access, modification, or deletion of audit information. [AU-9 (b)] Only the {Insert Information Security Team Name} has administrative access to {Insert Security Information and Event Management (SIEM) tool name}. The Information Technology team has permissions to administer the underlying {Insert Security Information and Event Management (SIEM) tool name} workspace. [AU-9 (4)]

### Audit Log Retention

{Insert Company Name} has configured {Insert Security Information and Event Management (SIEM) tool name} to retain logs and events for 365 days online. {Insert Security Information and Event Management (SIEM) tool name} provides support for after-the-fact investigations and security incidents. {Insert Company Name} uses {Insert Security Information and Event Management (SIEM) tool name} scaling to maintain adequate space to meet the retention requirements. [AU-11]

* 1. **Audit Generation [AU-12]**

The {Insert Product Name} Information System through {Insert Security Information and Event Management (SIEM) tool name} and {Insert Security Information and Event Management (SIEM) tool name} provides audit record generation capability. [Au-12 (a)] The {Insert Security Information and Event Management (SIEM) tool name} dashboards allow the {Insert Information Security Team Name} and {Insert Information Technology Team Name} Management to alter the level of alerting, and select which events are to be audited, based on the needs of organizational elements that require audit information. [AU-12 (b)] This is done by assessing the current threat landscape and ensuring that the selected auditable events are reviewed and updated appropriately.

{Insert Security Information and Event Management (SIEM) tool name} captures and {Insert Security Information and Event Management (SIEM) tool name} correlates all syslogs, application logs, and security logs from components within the authorization boundary. All logs captured are structured in accordance with the industry-standard syslog audit log format and include information about the events defined in AU-2(a) (Section 8.2 above) to include the type of event that occurred, when the event occurred, what component the event occurred on, the source of the event, the outcome (success or failure) of the event, and identities of any users associated with the event. [AU-12 (c)]