# Auditing and Accountability Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  |  | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage auditing of the secure enclave environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all audit procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME]. The CMMC System Security Plan (SSP) will be updated as these Auditing and Accountability procedures change.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME]
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.3.1 - 3.3.9
* CMMC AU.L2-3.1.1 – AU.L2-3.1.9
* [COMPANY NAME] – AU – 3.3 - Auditing and Accountability Policy

**Procedure Statements**

**AU.L2-3.3.1 - Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity:**

1. [COMPANY NAME] has defined the information system auditable events to support such monitoring, analysis, investigation, and reporting as:

* Logons and logoffs
* Access to security-relevant objects and directories, including creation, open, close, modification, and deletion
* Creation, modification, or deletion of user accounts or authenticators
* Creation, modification, or deletion of security RBAC roles or membership
* Blocking, disabling, or blacklisting of a user account or end user device
* Denial of access resulting from an excessive number of unsuccessful logons
* System audit events and/or modification or deletion of audit records
* Modification or deletion of system logs
* System configuration changes
* Modification to access control lists or policies

1. The content of audit records types as stated above supports monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Auditable events are identified in policy which much be captured on all [COMPANY NAME] systems and services. If these auditable events cannot be captured, then each system or service must be reviewed and approved by the <Role> before putting into operation. Each remote access request shall notify the end user upon connection. Remote access to all systems is limited to administrative users only and if another functional group requires the ability to remotely access a group of [COMPANY NAME] systems, then their access is restricted to only the least amount of assets that are needed operationally after approval from the CISO.
2. The information system, to include the Active Directory, user workstations, servers, virtual workstations, virtual servers, (firewall Name), VPN, automatically generate and maintain audit records to track significant system events and/or activity. All system audit logs are forwarded and collected in the organizational Microsoft Sentinel SIEM for monitoring, analysis, investigation, and reporting of unlawful or unauthorized information system activity.
3. Information systems are configured to identify the following events and contain the following information within the audit logs:

* User account ID or unique identifier used to initiate the event or action
* Type of event or action
* Subject or resource associated with the event or action
* Success or failure of the event or action
* Date of occurrence
* Time of occurrence
* Hostname, IP address, or other unique device identifier of the remote device from where the event or action was initiated

1. [COMPANY NAME] <Role> is required to retain Audit Records at a minimum of 1 year or when the memory allocated to audit logs is reached..
2. Audit records are retained in the <designated repository> which is limited using Azure AD RBAC to only allow Privileged users access.

**AU.L2-3.3.2 - Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions:**

1. <role> shall ensure that information systems are configured with Siem Solution to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
2. Audit records, once created, contain at a minimum the following elements that shall be identified within each audit record:
3. Date and time when the event occurred

2. The software or virtual component of the information system where the event occurred

3. Source of the event (e.g., network address, console)

4. Type of event that occurred

5. Subject identity (e.g., user, virtual machine, process context)

6. The outcome (i.e., success or failure) of the event

7. Security-relevant actions associated with processing

8. All boundary information system components are configured to comply with the guidance of all applicable industry standards.

**AU.L2-3.3.3 – Review and update logged events:**

1. [COMPANY NAME] reviews and updates the audited events Quarterly and based on situational awareness of threats and vulnerabilities. The review shall include coordination, research, or input from cybersecurity groups, associations, or consultants to determine if the list of auditable event types requires updating. Based upon the review, the <role> shall update the list of auditable event types if required, and document that the review has been completed.
2. [COMPANY NAME] reviews the listing of organization-defined audited events on an Quarterly basis. [COMPANY NAME] also generate and maintain an audit trail to document the completion of the review. Administrators have the ability to increase the frequency of events that are being monitored in the event of a change in risk based upon law enforcement, the situational awareness of threats or vulnerabilities, intelligence, security demands or other credible sources of information.
3. [COMPANY NAME] updates the listing of organization-defined audited events on an Quarterly l basis. [COMPANY NAME] also generate and maintain an audit trail to document the completion of the update actions. Administrators have the ability to increase the frequency of events that are being monitored in the event of a change in risk based upon law enforcement, the situational awareness of threats or vulnerabilities, intelligence, security demands or other credible sources of information.

* SIEM Solution provides the capability to centrally review and analyze audit records from multiple components within the system. <role> reviews the audit logs produced by SIEM Solution tool.

**AU.L2-3.3.4 – Alert in the event of an audit logging process failure:**

1. [COMPANY NAME] identifies the <role>, and <role> as key personnel to alert in the event of an audit processing failure.
2. If the cause is not readily apparent, the <role> will attempt to reproduce the audit failure, document the test case, and any identified causal conditions resulting in the failure of audit processing.
3. If the cause is apparent, the <role> will assess whether it was user-related, or a technical issue of the system/tool used.
4. If the audit failure is user-related, the <role> will update relevant documentation and any related training. If the audit failure is technical, the <role> will address the issue internally, and/ or work with vendor to resolve the failure.
5. Types of Audit logging process failures for which alert will be generated include:
   * Software and hardware errors or failure
   * Failures in audit log capturing mechanisms
   * Reaching or exceeding audit log storage capacity
6. [COMPANY NAME] information systems are configured to alert the <Role> in the event of an audit processing failure via automated alerts that are configured in the information system SIEM Solution.

**AU.L2-3.3.5** – **Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity:**

1. [COMPANY NAME] compiles audit records from all secure enclave information system and network components into a system-wide (logical or physical) audit trail that is time-correlated to within standards listed in AU.L2-3.3.7. [COMPANY NAME] has the capability to look across different pieces of the Information Technology System and be able to perform an analysis of events. If an alert is generated, then the <role> in conjunction with security administrators, will review the audit log information. Based on the review, if there is indication of malicious activity then the <role> will work in conjunction with security administrators to investigate and remediate any determined issues. Elevation of alert notification to the CEO resides with the MIS Manager based upon impact of the event.

* + [COMPANY NAME] will ensure that information systems that perform auditing are synced to the Microsoft central time source to ensure all contained timestamps are correlated.

1. <role> analyzes and correlates audit records across different repositories (firewall, applications, IPS, IDS, AV, and any other pertinent logs) to gain organization-wide situational awareness. [COMPANY NAME] ensures each members is available from the information system team to analyze, review, and correlate audit record investigations and information.

**AU.L2-3.3.6** – **Provide audit record reduction and report generation to support on-demand analysis and reporting:**

1. The information system is configured provide an audit reduction capability through the use of the SIEM Solution. Audit record reduction is an automated process that interprets raw audit log data and extracts meaningful and relevant information without altering the original logs.
   * [COMPANY NAME] provides an audit reduction capability that supports on-demand audit review and analysis, as well as after-the fact investigations of security incidents.
   * Audit reduction capability does not alter original content or time ordering of audit records.
2. The information system provides report generation capability through the use of the SIEM Solution. This tool supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and does not alter the original content or time ordering of audit records.

* [COMPANY NAME] provides the capability to filter audit records for events of interest based upon all audit fields within audit records based upon the following minimum criteria: Users: e.g., specific users or groups Event types: Event dates and time: System resources involved: e.g., application components or modules. IP addresses: Information objects accessed: Event level categories: e.g., high, critical, warning, error Key words: e.g., a specific search string.
* [COMPANY NAME] processes audit records for events of interest based on organization-defined audit fields within the audit records. Such as but not limited to; the identities of individuals, event types, event locations, event times, event dates, system resources involved, Internet Protocol addresses involved, or information objects accessed.
* [COMPANY NAME] provides the capability to sort and search audit records (reduce) for events of interest based on the content.

**AU.L2-3.3.7** – **Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records:**

1. The information system uses Microsoft to generate time stamps for audit records; and records time stamps for audit records.
2. [COMPANY NAME] has defined the authoritative time source as Microsoft time servers as designated for the appropriate DoD networks.
3. [COMPANY NAME] will configure the information system to use internal system clocks to generate and maintain accurate timestamps on all information system devices, to meet a one second granularity of time measurement. [COMPANY NAME] has defined the granularity of time measurement as one second for time stamps generated for audit records. [COMPANY NAME] configures the information system to generate timestamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

**AU.L2-3.3.8** - **Protect audit information and audit logging tools from unauthorized access, modification, and deletion:**

This control has been identified as deficient and has been placed on the PO&AM to become compliant. Once a solution is found, this procedure is to be created

1. [COMPANY NAME] has configured the information system to protect audit information from unauthorized access using Azure AD RBAC.
2. [COMPANY NAME] has configured the information system to protect audit information from unauthorized modification using Azure AD RBAC.
3. [COMPANY NAME] has configured the information system to protect audit information from unauthorized deletion using Azure AD RBAC.
4. [COMPANY NAME] has configured the information system to protect audit tools from unauthorized access using Azure AD RBAC.
5. [COMPANY NAME] has configured the information system to protect audit tools from unauthorized modification using Azure AD RBAC.
6. [COMPANY NAME] has configured the information system to protect audit tools from unauthorized deletion using Azure AD RBAC.

* Only User accounts other than those assigned to the Administrator role are not authorized to access, modify, or delete audit information or audit logging tools. The information system is configured via Microsoft Active Directory, such that accounts not assigned to the Administrator role, for example general users assigned to the User role, are administratively prevented from accessing, modifying, or deleting audit information and/or audit logging tools.
* Administrator role members are authorized and able to access audit information, perform audit functions, and utilize audit logging tools on the system, including access, modification, and deletion.

**AU.L2-3.3.9** **- Limit management of audit logging functionality to a subset of privileged users:**

1. [COMPANY NAME] has a subset of privileged users with authorized access to the management features of the audit functionality. Privileges will be given to these users in written form to perform their duties as auditors of the information system. Any specialized access (i.e. System Administrators, etc.) will be noted. Management is secured to single security group to ensure access of logs and audit functions. Non-privileged user accounts will not have access to any audit logging management console in the secure enclave. All access to the audit logging configuration is restricted to only *3* organizational roles:
   1. *<ISSO>*
   2. *<role>*
   3. *<role>*
2. [COMPANY NAME] authorizes access to management of audit functionality to only auditors and authorized privileged users.

**Roles and Responsibilities**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

**Non-Compliance**

Violations of this procedure will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 12/7/2022 | SecureStrux | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |