|  |  |  |
| --- | --- | --- |
| Policy #: | Title: | Effective Date: |
| x.xx | Auditing and Accountability Policy | MM/DD/YYYY |

PURPOSE
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCE
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Auditing and Accountability (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100

POLICY
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This policy is applicable to all departments and users of IT resources and assets.

1. AUDIT EVENTS

The information systems owners, in cooperation with audits and IT, shall:

1. Determine that the information system is capable of auditing the following events: [entity defined auditable events]
2. Coordinate the security audit function with other organizational entities requiring audit.
3. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
4. Determine that the following events are to be audited within the information system:
5. [entity defined auditable events].
6. REVIEWS AND UPDATES
7. The organization shall review and update the audited events [entity defined frequency].
8. CONTENT OF AUDIT RECORDS
9. The information system shall generate audit records containing information that establishes 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.
10. ADDITIONAL AUDIT INFORMATION
11. The information system shall generate audit records containing the following additional information: [entity defined additional, more detailed information].
12. AUDIT STORAGE CAPACITY
13. The information owner shall ensure audit record storage capacity is allocated in accordance with [entity defined audit record storage requirements].
14. TRANSFER TO ALTERNATE STORAGE
15. The information system shall off-load audit records [entity defined frequency] onto a different system or media than the system being audited.
16. RESPONSE TO AUDIT PROCESSING FAILURES

The information system shall:

1. Alert [entity defined personnel or roles] in the event of an audit.
2. Take the following additional actions: [entity defined actions to be taken processing failure; and (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
3. AUDIT STORAGE CAPACITY
4. The information system shall provide a warning to [entity defined personnel, roles, and/or locations] within [entity defined time period] when allocated audit record storage volume reaches [entity defined percentage] of repository maximum audit record storage capacity.
5. REAL-TIME ALERTS
6. The information system shall provide an alert in [entity defined real-time period] to [entity defined personnel, roles, and/or locations] when the following audit failure events occur:
	1. [entity defined audit failure events requiring real-time alerts].
7. CONFIGURABLE TRAFFIC VOLUME THRESHOLDS
8. The information system shall enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and rejects or delays network traffic above those thresholds.
9. SHUTDOWN ON FAILURE
10. The information system shall invoke a [full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available] in the event of [entity defined audit failures], unless an alternate audit capability exists.
11. AUDIT REVIEW, ANALYSIS, AND REPORTING

The information system owner shall:

1. Review and analyze information system audit records [entity defined frequency] for indications of [entity defined inappropriate or unusual activity].
2. Report findings to [entity defined personnel or roles].
3. PROCESS INTEGRATION
4. The information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
5. AUDIT REPOSITORIES
6. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness.
7. AUDIT REDUCTION AND REPORT GENERATION
8. The information system shall provide an audit reduction and report generation capability that:
9. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.
10. Does not alter the original content or time ordering of audit records.
11. AUTOMATIC PROCESSING
12. The information system shall provide the capability to process audit records for events of interest based on [entity defined audit fields within audit records].
13. TIME STAMPS

The information system shall:

1. Use internal system clocks to generate time stamps for audit records.
2. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [entity defined granularity of time measurement].
3. SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

The information system shall:

1. Compare the internal information system clocks [entity defined frequency] with [entity defined authoritative time source].
2. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [entity defined time period].
3. PROTECTION OF AUDIT INFORMATION
4. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.
5. ACCESS BY SUBSET OF PRIVILEGED USERS
6. The organization shall authorize access to management of audit functionality to only [entity defined subset of privileged users].
7. AUDIT RECORD RETENTION
8. The information system owners shall retain audit records for [entity defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
9. LONG-TERM RETRIEVAL CAPABILITY
10. The information system owners shall employ [entity defined measures] to ensure that long-term audit records generated by the information system can be retrieved.
11. AUDIT GENERATION

The information system shall:

1. Provide audit record generation capability for the auditable events as defined at [entity defined information system components].
2. Allow [entity defined personnel or roles] to select which auditable events are to be audited by specific components of the information system.
3. Generate audit records for the events with the content as defined. [entity defined information system components].
4. TIME-CORRELATED AUDIT TRAIL
5. The information system shall comply with audit records from [entity defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [entity defined level of tolerance for relationship between time stamps of individual records in the audit trail].
6. STANDARDIZED FORMATS
7. The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.
8. CHANGES BY AUTHORIZED INDIVIDUALS
9. The information system shall provide the capability for [entity defined individuals or roles] to change the auditing to be performed on [entity defined information system components] based on [entity defined selectable event criteria] within [entity defined time thresholds].

COMPLIANCE
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |