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:

a. Determine that the information system is capable of auditing the following events: user logon/logoff activities, access to sensitive or cardholder data, use of privileged accounts, system configuration changes, failed authentication attempts, firewall or access control modifications, creation or deletion of user accounts, and access to audit logs.

b. Coordinate the security audit function with other organizational entities requiring audit.

c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

d. Determine that the following events are to be audited within the information system:

   i. All user authentication events (successful and failed logins)
   ii. Use of root/admin or other privileged accounts
   iii. Access to and modification of cardholder data
   iv. Changes to firewall and router configurations
   v. Security group and access control modifications
   vi. Start/stop of audit logs
   vii. Application-level access to sensitive transactions

viii. Changes to system time or audit settings

2. REVIEWS AND UPDATES

    a. The organization shall review and update the audited events at least annually and whenever there is a significant change to the information system, threat environment, or compliance requirements, to ensure alignment with security objectives and regulatory obligations.

3. CONTENT OF AUDIT RECORDS

    a. 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.

4. AUDIT STORAGE CAPACITY

    a. The information owner shall ensure audit record storage capacity is allocated in accordance with retention requirements of at least 12 months, with a minimum of 3 months of logs readily available for analysis.

5. TRANSFER TO ALTERNATE STORAGE

    a. The information system shall off-load audit records daily onto a different system or media than the system being audited.

6. RESPONSE TO AUDIT PROCESSING FAILURES
   The information system shall:

    a. Alert the IT Security Team, System Administrator, and SOC (Security Operations Center) in the event of an audit.

7. AUDIT STORAGE CAPACITY

    a. The information system shall provide a warning to the IT Security Team and System Administrator within 5 minutes when allocated audit record storage volume reaches 80% of the repository’s maximum audit record storage capacity.

8. REAL-TIME ALERTS

a. The information system shall provide an alert in in real-time (within 1 minute) to the Security Operations Center (SOC), IT Security Team, and System Administrators when the following audit failure events occur:

    i. Failure to write audit logs due to full disk or permission issues
    ii. Unexpected termination or crash of the logging service (e.g., syslog, journald, Splunk forwarder)
    iii. Tampering or deletion of audit records
    iv. Failure to synchronize system time (which may impact log accuracy)
    v. Unauthorized access attempts to the log storage directory
    vi. Detection of log forwarding interruption (e.g., logs no longer reaching central SIEM).

9. CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

    a. 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.

10. SHUTDOWN ON FAILURE

    a. The information system shall invoke a degraded operational mode with limited mission/business functionality available in the event of critical audit failures such as the inability to write logs, detect log tampering, or loss of connection to the centralized logging system, unless an alternate audit capability exists.

11. AUDIT REVIEW, ANALYSIS, AND REPORTING
    The information system owner shall:

    a. Review and analyze information system audit records weekly, and immediately following a security incident, for indications of unauthorized access, privilege misuse, abnormal login patterns, data exfiltration, system configuration changes, or other suspicious activity.

    b. Report findings to the Chief Information Security Officer (CISO), IT Security Team, and Internal Audit for further investigation and potential remediation actions.

12. PROCESS INTEGRATION

    a. 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.

13. AUDIT REPOSITORIES

a. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness.

14. AUDIT REDUCTION AND REPORT GENERATION

    a. The information system shall provide an audit reduction and report generation capability that:

        i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.

        ii. Does not alter the original content or time ordering of audit records.

15. AUTOMATIC PROCESSING

    a. The information system shall provide the capability to process audit records for events of interest based on fields such as user ID, source/destination IP address, event type, timestamp, resource accessed, and status code (success/failure).

16. TIME STAMPS
    The information system shall:

a. Use internal system clocks to generate time stamps for audit records.

b. Record timestamps of audit records that can be mapped to West African Coordinated Time (WAT) and that respond to a granularity of one second or finer.

17. SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
    The information system shall:

a. Compare the internal information system clocks at least every 6 hours with an authoritative NTP time source.

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 5 seconds.

18. PROTECTION OF AUDIT INFORMATION

    a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

19. ACCESS BY SUBSET OF PRIVILEGED USERS

a. The organization shall authorize access to management of audit functionality to only Security Administrators and Internal Audit personnel designated by the CISO.

20. AUDIT RECORD RETENTION

a. The information system owners shall retain audit records for at least 1 year, with a minimum of 3 months immediately available for analysis, to support after-the-fact investigations of security incidents and to meet regulatory and organizational retention requirements.

21. LONG-TERM RETRIEVAL CAPABILITY

a. The organization shall employ centralized log archiving with indexing, metadata tagging, and backup to WORM (Write Once, Read Many) storage to ensure that long-term audit records can be retrieved.

22. AUDIT GENERATION
The information system shall:

a. Provide audit record generation capability for the auditable events as defined at all network, application, database, and system components.

b. Allow Security Administrators to select which auditable events are to be audited by specific components of the information system.

c. Generate audit records for the events with the content as defined in the organization's audit log schema (e.g., including user ID, timestamp, source IP, event type) across critical systems, servers, firewalls, and applications.

23. TIME-CORRELATED AUDIT TRAIL

a. The information system shall compile audit records from network devices, applications, operating systems, and databases into a system-wide (logical or physical) audit trail that is time-correlated to within 1 second across all components.

24. STANDARDIZED FORMATS

a. The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

25. CHANGES BY AUTHORIZED INDIVIDUALS

a. The information system shall provide the capability for Security Administrators and System Owners to change the auditing to be performed on firewalls,

application servers, and domain controllers based on event severity, asset classification, or threat level within 24 hours of change approval.

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