|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Auditing and Accountability** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

# The purpose of this policy is to ensure that IT resources and information systems are equipped with comprehensive security controls to monitor, audit, and respond to system activities, thereby maintaining compliance with federal and state laws, Executive Orders, regulations, and internal organizational policies. This policy aims to preserve the integrity, confidentiality, and availability of critical information assets through regular assessments of security measures and systematic capture of audit events.

# The benefits of this policy are multifaceted. It enhances security by enabling proactive monitoring of system activities, allowing for early detection of unauthorized access and other anomalies. By establishing clear audit requirements, it ensures accountability, providing a basis for investigations and responses to security incidents.

# Regular audits also facilitate compliance with legal and regulatory standards, reducing the risk of penalties. Moreover, the policy supports operational efficiency by ensuring that audit processes are integrated into organizational workflows, allowing for timely analysis and reporting of suspicious activities. Ultimately, it fosters a culture of security awareness and diligence, reinforcing the organization’s commitment to protecting its information assets.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

This policy ensures that IT resources and information systems are equipped with security controls designed to monitor, audit, and respond to system activities in accordance with federal and state laws, regulations, and internal organizational policies. This approach aims to maintain the integrity, confidentiality, and availability of critical information assets by regularly assessing the security measures in place, capturing audit events, and ensuring continuous compliance with established security standards.

### 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:
   1. Login Attempts
   2. Data Access
   3. Data Downloads
   4. File Modifications
   5. System Failures
   6. Configuration Changes
   7. Priviliege Escalations
   8. Policy Violations
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:
   1. Login Attempts
   2. Data Access
   3. Data Downloads
   4. File Modifications
   5. System Failures
   6. Configuration Changes
   7. Priviliege Escalations
   8. Policy Violations
   9. Reviews and Updates

The organization shall review and update the audited events annually.

* 1. Content of Audit Records

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.

* 1. Additional Audit Information

The information system shall generate audit records containing the following additional, more detailed information:

1. IP Addresses
2. Session Identifiers
3. Application-level Logging
   1. Audit Storage Capacity

The information owner shall ensure audit record storage capacity is allocated in accordance with the organization's data retention policy.

* 1. Transfer to Alternate Storage

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

* 1. Response to Audit Processing Failures

The information system shall:

1. Alert [owner] in the event of an audit processing failure.
2. Take the following sequential actions, if needed:
   1. Shut down information system
   2. Overwrite oldest audit records
   3. Stop generating audit records
   4. Audit Storage Capacity

The information system shall provide a warning to [owner] within 24 hours when allocated audit record storage volume reaches 85% of repository maximum audit record storage capacity.

* 1. Real-Time Alerts

The information system shall provide an alert in real-time to the security operations center when the following audit failure events occur:

1. Unauthorized access attempts
2. Audit log deletion attempts
   1. Configurable Traffic Volume Thresholds

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.

* 1. Shutdown on Failure

The information system shall invoke a partial system shutdown in the event of a system-wide audit failure, unless an alternate audit capability exists.

* 1. Audit Review, Analysis, and Reporting

The information system owner shall:

1. Review and analyze information system audit records monthly for indications of suspicious or unusual activity.
2. Report findings to [Authority]
   1. Process Integration

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.

* 1. Audit Repositories

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

* 1. Audit Reduction and Report Generation

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

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.
2. Does not alter the original content or time ordering of audit records.
   1. Automatic Processing

The information system shall provide the capability to process audit records for events of interest based on security-relevant fields within audit records.

* 1. 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 meet millisecond-level granularity of time measurement.
   1. Synchronization with Authoritative Time Source

The information system shall:

1. Compare the internal information system clocks weekly with the National Institute of Standards and Technology (NIST) time servers.
2. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 2 seconds.
   1. Protection of Audit Information

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

* 1. Access by Subset of Privileged Users

The organization shall authorize access to management of audit functionality to only senior system administrators and security analysts.

* 1. Audit Record Retention

The information system owners shall retain audit records for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

* 1. Long-Term Retrieval Capability

The information system owners shall employ cloud-based storage solutions to ensure that long-term audit records generated by the information system can be retrieved.

* 1. Audit Generation

The information system shall:

1. Provide audit record generation capability for the auditable events as defined at network gateways, databases, and user authentication systems.
2. The information system shall allow security analysts to select which auditable events are to be audited by specific components of the information system.
3. The information system shall generate audit records for the events with the content as defined in key system components.
   1. Time-Correlated Audit Trail

The information system shall compile audit records from all core systems into a system-wide (logical or physical) audit trail that is time-correlated to within 10 milliseconds for consistency across platforms.

* 1. Standardized Formats

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

* 1. Changes by Authorized Individuals

The information system shall provide the capability for authorized security personnel to change the auditing to be performed on core network components based on detected threat levels within 5 minutes of escalation.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publication 800-92, Guide to Computer Security Log Management](https://csrc.nist.gov/publications/detail/sp/800-92/final" \t "_blank)

[National Institute of Standards and Technology (NIST) Special Publication 800-53a, Assessing Security and Privacy Controls in Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/53/a/r5/final)