|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Auditing and Accountability Policy** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

# 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.

# 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 users of any system’s information or physical infrastructure regardless of its form or format, created or used to support the organization. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organization’s Information Security Policy and its associated standards.

# 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

* 1. The information systems owners, in cooperation with audits and IT, shall determine that the information system is capable of auditing the following events: login attempts, data access, file modifications, system failures, and configuration changes.
  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: data downloads, privilege escalations, and policy violations.

### Reviews and Updates

1. The organization shall review and update the audited events annually.

### Content of Audit Records

1. 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.

### Additional Audit Information

1. The information system shall generate audit records containing the following additional, more detailed information: IP addresses, session identifiers, and application-level logging.

### Audit Storage Capacity

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

### Transfer to Alternate Storage

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

### Response to Audit Processing Failures

1. Alert [owner] in the event of an audit processing failure.
2. Take the following additional actions: trigger an alert to the security operations team and initiate log rotation when storage is 90% full.

### Audit Storage Capacity

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

### Real-Time Alerts

1. The information system shall provide an alert in real-time to the security operations center when the following audit failure events occur: unauthorized access attempts and audit log deletion attempts.

### Configurable Traffic Volume Thresholds

1. 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.

### Shutdown on Failure

1. The information system shall invoke a degraded operational mode with limited mission/business functionality available in the event of a system-wide audit failure, unless an alternate audit capability exists.

### Audit Review, Analysis, and Reporting

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

### Process Integration

1. 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.

### Audit Repositories

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

### Audit Reduction and Report Generation

1. The information system shall provide an audit reduction and report generation capability that: Supports on-demand audit review, analysis, and reporting requirements and after-the-fact. Does not alter the original content or time ordering of audit records.

### Automatic Processing

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

### Time Stamps

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.

### Synchronization with Authoritative Time Source

1. The information system shall compare the internal information system clocks weekly with the National Institute of Standards and Technology (NIST) time servers.
2. The information system shall synchronize the internal system clocks to the authoritative time source when the time difference is greater than 2 seconds.

### Protection of Audit Information

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

### Access by Subset of Privileged Users

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

### Audit Record Retention

1. 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.

### Long-Term Retrieval Capability

1. 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.

### Audit Generation

1. The information system shall 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.

### Time-Correlated Audit Trail

1. 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.

### Standardized Formats

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

### Changes by Authorized Individuals

1. 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

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

# 10.0 Related Documents

[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 Publications (SP): NIST SP 800-53a – Auditing and Accountability (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100