Audit Trails Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Audit trails can help detect security violations, performance issues, and flaws in applications. They can also be used to help reconstruct or review Information Resource related activities.

# II. Purpose

This policy establishes the framework for audit trails and their use as a technical control to help manage Information Resource related risks.

# III. Scope

This policy applies to the IT Department and other departments responsible for acquiring, implementing, and maintaining Information Resources.

# IV. Policy

A. Purpose

An Information Resources audit trail is a record of activities and events related to IT facilities, networks, servers, users, applications, and related assets. An Information Resource may have different types of audit trails each devoted to a particular activity.

Auditing includes the review and analysis of safeguards and controls. In many instances audit trails are used as record of activity. Auditing systems generally consist of:

* Logging – collecting and recording events
* Reporting – data analyzer and reporting

Often a file is used to transfer the audit data from the collector to the analyzer. This leads to problems when the audit data is collected from different systems. This is due to the lack of a standard interface for audit trails. Developing standards for the format and content of audit trails is an ongoing research effort.

Audit trails can be used:

* To establish individual accountability – an individual's actions are tracked in an audit trail allowing users to be personally accountable for their actions. With user actions logged, audit trails help ensure accountability and Staff are less likely to perform unauthorized activities. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions.
* Reconstruct events – audit trails can be used to reconstruct events after an incident has occurred. The amount of damage that occurred can be assessed by reviewing audit trails of system activity to identify how, when, and why the incident occurred.
* Resource monitoring (problem identification) – audit trails may also be used to detect disk failures, over utilization of system resources, network outages, and similar events.
* Intrusion detection – audit trails can help determine events that allowed unauthorized access to Information Resources. Intrusions can be detected in real time, by examining audit records as they are created or after the fact, by examining audit records in a batch process. Deploying, monitoring, and reporting are important intrusion detection considerations.

Monitoring systems and audit trails shall be used to prevent unauthorized personnel from accessing ABC Company’s Information Resources. Audit trails can also be used as an incident detection and response mechanism to:

* Reconstruct a timeline of events that occurred
* Identify individuals involved
* Additional information for research into the extent of the damage
* Help ensure correction
* Resume normal business operations with minimal delay
* Use information from this incident to minimize or eliminate future events

The Risk Assessment Policy ensures that important assets are identifies and the appropriate security controls are in place. Real time monitoring shall be used on important Information Resources to ensure their continued availability and integrity.

B. Audit Trail Requirements

Information Resources shall automatically create and maintain audit trails or logs. Refer to the Logging Policy for more information on:

* Activities to be logged
* Elements of the log
* Log formatting and storage
* Log information security issues
* Where possible, audit trails shall include before and after versions of records that were modified. This allows ABC Company to reconstruct events whether the event was made by a Staff member, a hardware malfunction, software bug, etc.

Audit trails created and maintained by the information system shall record changes to user formal access permissions. Monitoring and logging activities shall include the unique identification of each user and association of that identity with all auditable actions taken by that individual.

Information Resources clocks shall be synchronized to enable research and investigation activities.

Sensitive Information shall be sanitized before being written to log files.

Monitoring and logging activities shall be periodically tested by IT security Staff.

C. Review and Analysis

Audit trails must be reviewed on a daily basis. Such review to include a review of:

* All security events
* Logs of all system components that store, process, or transmit sensitive information or could impact the security of sensitive information.
* Logs of all critical system components.
* Logs of all servers and system components that perform security functions (e.g. firewalls, intrusion detection systems (IDS), intrusion-prevention systems (IPS), authentication servers, e‑commerce redirection servers, etc.).
* Review of logs of other system components periodically based on ABC Company’s risk management strategy, as determined by the annual risk assessment.

Staff shall be assigned to follow-up on all exceptions and anomalies identified during the review process.

Log files shall be copied to a protected area and retained for at least one year to assist in future investigations and monitoring. At least three months of history shall be immediately available for analysis (e.g. on-line, archived, or restorable from backup).

The following must be considered when reviewing audit trails:

* Recognize normal activity – reviewers must know what to look for to be effective in spotting unusual activity. They need to understand patterns and activity of normal traffic.
* Recognize unusual activity – Staff shall review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this requirement.
* Contain a search capability – audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.
* Follow-up reviews – the appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.
* Develop review guidelines – application owners, data owners, system administrators, data processing function managers, and computer security managers must determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.
* Automated audit analysis – analysis and reporting shall be performed using automated tools on a scheduled basis. Monitoring systems and logs shall be reviewed and analyzed in a timely manner. Log files related to file integrity, IDS, IPS, authentication, and authorization systems shall be reviewed and analyzed daily.

D. Security Considerations

The contents of audit trails shall be protected against unauthorized access, modification, or deletion. IT security Staff must protect the audit trail from unauthorized access. The following precautions must be taken:

* Control online audit logs. Access to online audit logs must be strictly controlled.
* Separation of duties. The Company strives for separation of duties between various personnel who administer the access control function and those who administer the audit trail.
* Protect confidentiality. The confidentiality of audit trail information must be protected if, for example, it records personal information about users.

Access to monitoring systems and log files shall be restricted to authorized personnel and protected against unauthorized alteration. File integrity monitoring or change detection software shall issue alerts upon unauthorized modification of:

* Critical system files
* Configuration files
* Log files

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all IT Department personnel and other ABC Company Staff members responsible for acquiring, implementing, and maintaining Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM02.03, EDM03.02, APO01.11, APO12.07, BAI04.05, MEA03.01, MEA04.11

GDPR Article 30, 32

HIPAA 164.308(a)(1)(ii)(D)

ISO 27001 A.12.4, A.15.2

NIST SP 800-37 3.7

NIST SP 800-53 3.4, AU-12, AU-13

NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2

PCI 6.3, 6.4.6, 10