Logging 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

This policy provides guidelines on the monitoring and logging of ABC Company’s Information Resources including ABC Company’s network and communications systems.

# II. Purpose

This policy is established to protect the integrity, availability and confidentiality of information, to prevent loss of service, and to comply with legal requirements. This policy ensures that all Information Systems generate appropriate audit logs.

# III. Scope

This policy applies to all ABC Company IT system administrators, IT security Staff, the IT Director, and the Chief Security Officer.

# IV. Policy

Without frequent monitoring and logging, it is difficult to assess the effectiveness of access controls. Unauthorized access can remain undetected, enabling information to be disclosed to persons with possible malicious or fraudulent intent.

Access to ABC Company’s network and communications shall be logged and monitored to identify potential misuse of systems or information. System access must be monitored regularly to prevent attempts at unauthorized access and to confirm that access control systems are effective.

Logs shall be kept secure and are only available to personnel authorized by IT Management. Such logs shall only be kept as long as necessary as outlined in ABC Company’s Data Retention Policy.

ABC Company’s information Systems shall be monitored and logged:

* Ensure use is authorized
* Manage and administer of systems
* Protect against unauthorized access
* Verify security procedures
* System and operational security
* Comply with ABC Company’s policies and procedures
* Detect and prevent crime
* Identify, report, and correct information and Information Systems flaws in a timely manner

A. Underlying requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit logging information:

* Determine the activity that was performed
* Who or what performed the activity, including where or on what system the activity was performed (subject)
* Systems involved (object)
* When the activity was performed
* Tools used
* The status (such as success vs. failure), outcome, or result of the activity

The IT Director shall ensure that local logging has been enabled on all systems and networking devices. The Chief Security Officer (CSO) shall ensure that a centralized logging server has been implemented, configured, and all critical devices log to the server. The IT Director shall ensure important events and audit trials are logged for analysis and review. A file integrity monitoring/change detection software shall review logs and issue alerts if the log data is altered.

B. Activities to be logged

If audit trail reports and event logs are not regularly reviewed, incidents can remain undetected. IT staff shall be assigned to review and monitor the logs. Logs shall be reviewed on a regular and on-going basis. The frequency review shall be according to the sensitivity of the information stored and maintained. Procedures should verify that logging is active and working properly:

* Ensure events are properly classified
* Review logging for performance delays
* Ensure compliance related logging cannot be “turned off”
* Verify access to log files is properly restricted
* To assist with investigations, all critical system clocks and times should have their date and time synchronized using Network Time Protocol (NTP)
* Time data shall be protected and time settings shall be received from industry accepted time sources

System events shall be logged at the time activities are to be performed:

* System start up, restart, or shut down
* Application process startup, restart, or shutdown
* Read, write, update, or delete authentication information (e.g. IDs, passwords)
* Initiate or accept a network connection
* Grant, modify, or terminate access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes
* System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
* Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault
* Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system

Access to information shall be logged:

* Read, write, update, or delete Sensitive Information
* User authentication and authorization such as user login and logout
* Read, write, update, or delete information identified by the Chief Security Officer (CSO) as needing to be logged

The CSO shall implement automated audit trails for all Information Systems and components to reconstruct the following events:

* All individual user accesses to sensitive information
* All actions taken by any individual with root or administrative privileges
* Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
* Access to all audit trails
* Invalid logical access attempts
* Initialization, stopping, or pausing of the audit logs
* Creation and deletion of system level objects

C. Elements of the log

System events and activities that should be monitored and logged include:

* System administrator and system operator activities
* System start-ups and shut-downs
* Logging start-ups and shut-downs
* Backups
* Exceptions
* Security events
* Protection software
* Protection hardware (firewalls, routers, etc.)
* Intrusion Detection Systems (IDS) and Intrusion Prevention Systems
* Modifications to data characteristics including permissions, location, file type
* Authentication successes and failures (e.g. log in, log out, failed logins)

Application logging requires more than just relying on server logs. Application logs help identify security incidents, establish baselines, providing information about problems and unusual conditions, assist with incident investigation, and help detect attacks. Application events and activities that should be monitored and logged include:

* Application authentication (e.g. successes, failures, logouts)
* Data audit trails (e.g. access to sensitive data, adding data, modifying data, deleting data, exporting and importing data)
* Input validation failures (e.g. protocol violations, unacceptable encodings, invalid parameter names and values)
* Output validation failures (e.g. database record mismatch, invalid data encoding)
* Suspicious behavior (e.g. multiple records deleted in a short period of time, invalid access attempts)
* Session management failures (e.g. cookie session identification value modification)
* Application errors and events (e.g. syntax and runtime errors, connectivity problems, third party service error messages, file system errors, sequencing failure)
* Higher-risk functionality (e.g. network connections, adding and deleting users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of administrative privileges, access by application administrators, access to sensitive data, use of data encrypting keys, key changes, creating and deleting system-level objects, data import and export including screen-based reports, submission of user-generated content)
* Legal and other opt-ins (e.g. permissions to access credit history, terms of use, permission to receive marketing communications)
* Security events or warnings

Log entries and automated audit trails should include:

* Host name, system component, or resource
* Date
* Time
* Application ID (e.g. name and version)
* Initiating process or origination of event (e.g. entry point URL, page, form)
* Code location (e.g. module, subroutine)
* User initiating action (e.g. user ID)
* Event type
* Result status (e.g. success, failure, defer)
* Resource (e.g. identity or name of affected data, component)
* Location (e.g. IP address or location)
* Severity of event (e.g. emergency, alert, fatal error, warning, information only)
* Other (e.g. parameters, debug information, system error message)

D. Formatting and storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

* Microsoft Windows Event Logs should be collected by a centralized log management system
* Logs should be stored in a documented format and sent via reliable network protocols to a centralized log management system
* Logs stored in a SQL database that itself generates audit logs in compliance with the requirements of this Policy
* Other open logging mechanisms supporting the above requirements

E. Information Security Issues

Logs are one of the primary tools used by Administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems. Detailed procedures that support this policy shall be developed to protect against log security risks such as:

* System administrators and those with operating system command line access can disable or circumvent access control and audit log mechanisms
* Staff with command line access can execute system commands that can damage and corrupt the system, data files, and/or log files
* The contents of system logs should be protected from unauthorized access, modification, and/or deletion; write once read many (WORM) drives may be an acceptable solution
* Emergency access to systems shall only be used in extreme circumstances and only when authorized by IT Management. Emergency access may by-pass traditional security controls and access to information resources or Company data shall be logged
* As a log approaches its maximum size, it can either overwrite old events or stop logging new events. This makes it susceptible to attacks in which an intruder can flood the log by generating a large number of new events. A partial defense against this is to increase the maximum log size so that a greater number of events is required to flood the log
* Administrators can change the auditing policies to stop logging an unauthorized activity. Log settings should be set to track and record log policy changes (audit policy change setting)
* Given the ability of administrators to manipulate log files to cover unauthorized activity, ABC Company IT Management shall ensure a separation of duties between operations and security monitoring. Frequent backups of the log to a server accessible only to the security monitoring staff can improve security
* Keeping the IT department's security systems and practices confidential helps prevent users from formulating ways to cover their tracks. If users are aware that the log is copied over to the remote log server at :00 of every hour, for instance, they may take measures to defeat that system by attacking at :10 and then deleting the relevant log events before the top of the next hour]
* If an Administrator account has been compromised, the event history, as contained in the log, is unreliable; a WORM drive or remote log server with all services disabled (allowing only console access) might be acceptable solutions

The CSO shall be responsible for:

* Ensuring a regular review of activity audit logs, access reports, and security incidents. Approving the types of logs and reports to be generated, review activities to be performed, and procedures that describe the specifics of the reviews
* Procedures that specify monitoring log-in attempts, reporting discrepancies, and processes used to monitor log-in attempts
* Procedures that specify audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information. Procedures ensure that the audit controls meet security requirements by recording and examining activity related to sensitive information
* Securing audit trails by limiting viewing of audit trails to those with a job-related need, protecting audit trail files from unauthorized modifications, ensuring audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, writing logs for external facing technologies onto a log server on the internal log server or media device, and using file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (new data being added should not cause an alert)
* Software activity involving critical assets and sensitive data is tracked. Attacks are detected and the impacts and effects of attacks are minimized

# V. Enforcement

Any Staff 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 system administrators, IT security Staff, the IT Director, and the Chief Security Officer.

**Policy History**

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

**References:**

COBIT EDM02.03, APO11.09, APO12.02, APO13.07, BAI04.05, BAI09.04, DSS01.05, DSS05.02

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(b), 164.312(b)

ISO 27001:2013 9.1, 9.3, A.12.1.3, A.12.4

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 3.4, AC-2, AC-8, AC-17, AU-6, AU-13, CA-7, CM-1

NIST Cybersecurity Framework PR.DS-4, DE.AE-1-4, DE.CM-1-6, DE.DP-2, RS.RP-1

PCI 6.3, 10.1-9, A1.3, A3.2.2.1, A3.3.1, PCI Software Security Framework