Logging Procedure

|  |  |
| --- | --- |
| 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 procedure provides guidelines on the monitoring and logging of ABC Company’s Information Resources including ABC Company’s network and communications systems.

# II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in ABC Company's Logging Policy.

# III. Scope

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

# IV. Procedure

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

Logs are secured and are only available to personnel authorized by IT Management. Logs are retained per ABC Company’s Data Retention Policy.

A. Underlying requirements

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

* The activity that was performed
* Who or what performed the activity
* Where and on what system the activity was performed
* Systems involved
* When the activity was performed
* Tools used
* The status (e.g. success, failure), outcome, and result of the activity

The IT Director ensures:

* Local logging has been enabled on all systems and networking devices
* A centralized logging server has been implemented, configured, and all critical devices log to the server
* Important events and audit trials are logged for analysis and review
* File integrity monitoring/change detection software reviews logs and issues alerts if the log data is altered

B. Activities to be logged

IT staff are assigned to review and monitor the logs. Logs are reviewed on a regular and on-going basis. The frequency review is according to the sensitivity of the information stored and maintained. Procedures verify that logging is active and working properly. Logging systems and log files are reviewed to ensure:

* Events are properly classified
* Performance delays are identified
* Compliance related logging cannot be “turned off”
* Access to log files is properly restricted
* All critical system clocks and times have their date and time synchronized using Network Time Protocol (NTP)
* Time data is protected and time settings are received from industry accepted time sources

System events logged at the time activities are performed include:

* 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, resource exhaustion or reaching a resource limit or threshold (e.g. 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 is logged and includes:

* 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 ensures automated audit trails for all Information Systems and components can 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, creating new accounts and elevation of privileges.
* 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
* Creating and deleting system level objects

C. Elements of the log

System events and activities 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 events and activities 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 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

Logging systems support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and support enterprise-level analysis and reporting:

* Microsoft Windows Event Logs are collected by a centralized log management system
* Logs are stored in a documented format and sent via reliable network protocols to a centralized log management system
* Logs are stored in a SQL database that itself generates audit logs in compliance with the requirements of this Procedure

E. Logging Security Controls

Logs are reviewed by Administrators to troubleshoot problems and detect and investigate attempted and successful unauthorized activity. Given the ability of Administrators to manipulate log files to cover unauthorized activity, ABC Company IT Management ensures a separation of duties between operations and security monitoring.

The CSO ensures:

* Log settings track and record log configuration changes
* Emergency access to systems is only used in extreme circumstances when authorized by IT Management
* A regular review of activity audit logs, access reports, and security incidents is performed.
* Proper types of logs, reports generated, and review activities
* Monitoring log-in attempts, reporting discrepancies, and processes used to monitor log-in attempts
* Audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information are reviewed and appropriate action taken
* Audit controls meet security requirements by recording and examining activity related to sensitive information
* Limiting viewing of audit trails to those with a job-related need
* Protecting audit trail files from unauthorized modifications
* Frequent backups of logs to a server accessible only to security monitoring staff
* Log files are promptly backed up to a centralized log server or media that is difficult to alter (e.g. WORK drive)
* File integrity monitoring or change detection software so log data cannot be changed without generating alerts
* 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 procedure may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This procedure is to be distributed to all IT system administrators, IT security Staff, the IT Director, and the Chief Security Officer.

**Procedure History**

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