|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Log Management and Monitoring Policy | | | | | |
| Policy # | CPL-15-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc384806628)

[Scope 1](#_Toc384806629)

[Policy 1](#_Toc384806630)

[Audit Log Planning 1](#_Toc384806631)

[Audit Logging Requirements 2](#_Toc384806632)

[Audit Log Contents 3](#_Toc384806633)

[Audit Log Composition 3](#_Toc384806634)

[Log Content Restrictions and Data Privacy 3](#_Toc384806635)

[Specific Logging Requirements 4](#_Toc384806636)

[Management 5](#_Toc384806637)

[Protection of Log Information 5](#_Toc384806638)

[Log Storage and Maintenance 5](#_Toc384806639)

[Clock Synchronization 6](#_Toc384806640)

[Example Roles and Responsibilities 6](#_Toc384806641)

[Violations 6](#_Toc384806642)

[Definitions 7](#_Toc384806643)

[References 8](#_Toc384806644)

[Related Documents 8](#_Toc384806645)

[Approval and Ownership 8](#_Toc384806646)

[Revision History 8](#_Toc384806647)

Purpose

This policy defines the requirements for managing and monitoring the logs that are generated by Company X computer and communications systems.

Scope

This policy applies to all Company X computer and communications systems, with a target audience of Company X Information Technology employees and partners.

Policy

### Audit Log Planning

**Roles and Responsibilities Definition** – Company X management must define and document the responsibilities of every person responsible for management of system logs.

**Log Management Training** – Company X management must provide information systems staff responsible for log management with proper training and tools to perform their jobs effectively.

**Log Management Infrastructure** – Company X management must provide the budget and tools necessary to support a log management infrastructure.

**System Logging Standards -** The Information Security Department is responsible for publishing an internal standard defining the nature of the information that must be recorded in computer and network device system logs. This information must be made securely network-accessible in order to support a variety of network security systems (such as intrusion detection systems).

**System Classification Requirements –** The Information Security Department must establish specific logging requirements appropriate for the classification of the system being logged. *(Note: You may include reference to the Five Category Systems Classification.)*

### Audit Logging Requirements

**Computer System Audit Logs** - Logs of computer security-relevant events must provide sufficient data to support comprehensive audits on the effectiveness of, and compliance with security measures.

**Communication Logging** – All electronic communications across Company X computer systems and networks, including electronic mail, instant messaging, and web usage must be recorded and logged.

**Sensitive Application Systems Logs** - All production application systems that handle sensitive Company X information must generate logs that capture every addition, modification, and deletion to such sensitive information.

**Physical Access Logging** - Company X will maintain logs of all physical access to protected areas, including electronic physical access systems, video monitoring and visitor access recorded on paper.

**Privileged System Command Accountability And Traceability** - All privileged commands issued by computer system operators must be traceable to specific individuals through the use of comprehensive logs.

**Systems Log And Audit Trail Disclosure** - Systems logs or application audit trails must be classified as CONFIDENTIAL and not be disclosed to any person outside the team of individuals who ordinarily view such information in order to perform their jobs or investigate information security incidents. All exceptions require the approval of the Information Security Manager.

**Log Management Procedures** –The information security department will develop log management procedures covering the following areas:

* Monitoring the logging status of all log sources
* Monitoring log rotation and archival processes
* Managing logging software, including version control for upgrades and patches, and acquiring, testing, and deploying them
* Logging host’s clock synchronization to a common time source
* Reconfiguring logging as needed based on policy changes, technology changes, and other factors
* Documenting and reporting anomalies in log settings, configurations, and processes.

### **Audit Log Contents**

**Computer and Communication System Logs** - All Company X multi-user production systems must have computer operator logs that record, at a minimum, production application start and stop times, system boot and restart times, system configuration changes, system errors and corrective actions taken.

### Audit Log Composition

(Option 1: High-level description of minimum logging standard)

**Production Application System Logs** - All computer systems running Company X production application systems must include logs that record, at a minimum, user session activity including user IDs, logon date and time, logoff date and time, as well as applications invoked, changes to critical application system files, changes to the privileges of users, and system start-ups and shut-downs.

**(Option 2**: Specific policy statements for each type of logging.)

**User Activity Logging -** All computer systems running Company X production application systems must include logs that record, at a minimum, user session activity including user IDs, logon date and time, logoff date and time.

**Logging Security-Relevant Events** - Computer systems handling Sensitive information must securely log all significant security relevant events including, but not limited to, password guessing attempts, attempts to use privileges that are not authorized, modifications to production application software, and modifications to system software.

**Logging Access Control Alarms** - Audit logs must be maintained on all Company X computer and communications systems that record the alarms raised by the access control system.

**Virus Protection Systems** - Audit logs must be maintained on all Company X computer and communications systems that record the activation and de-activation anti-virus systems and intrusion detection systems.

**Privileged System Commands** - All privileged commands issued by computer system operators must be traceable to specific individuals through the use of comprehensive logs.

**Privileged User ID Activity Logging** - All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs must be securely logged and reflected in periodic management reports.

**Logon Attempt Logging** - Whether successful or not, all user initiated logon attempts to connect with Company X production information systems must be logged.

**Log Access Logging** - Access to all system logs and audit trails on Company X computer and communications systems must be logged.

**Log Initialization Logging** - The initialization of all system logs and audit trails on Company X computer and communications systems must be logged.

**Application Systems Logging** - All Company X multi-user production systems must have computer operator logs that show production application start and stop times, system boot and restart times, system configuration changes, system errors and corrective actions taken, and confirmation that files and output were handled correctly.

### Log Content Restrictions and Data Privacy

**Recording Private Information in Logs** - Company X information systems must be configured so that they do not capture private information in audit trails or logs.

**Password Logging** - Unencrypted passwords, whether correctly typed or not, must never be recorded in system logs.

**Customer Activity Log Disclosure** - Logs reflecting the activities of computer users or those served by computers must not be disclosed to third parties unless Company X is compelled to do so by court order, law, or regulation, or in receipt of written approval from the involved individuals.

### Specific Logging Requirements

**Log Entry Composition - User Identification** - Every log and audit trail entry captured by a Company X computer or communication system must contain the identity of the user associated with the entry.

**Log Entry Composition - Successes and Failures** - Every log and audit trail entry captured by a Company X computer or communication system must contain success or failure indication associated with the entry.

**Log Entry Composition - Event Origination** - Every log and audit trail entry captured by a Company X computer or communication system must contain the origination of the entry.

**Log Entry Composition - Privileges** - Audit logs must be maintained on all Company X computer and communications systems that record the use of all privileges.

**Log Entry Composition - Systems Software Utilities** - Access to systems software utilities must be restricted to a small number of trusted and authorized users, and whenever these utilities are executed, the resulting activity must be securely logged, and later reviewed by the Computer Operations Manager.

**Log Entry Composition - Event Origination** - Every log and audit trail entry captured by a Company X computer or communication system must contain the origination of the entry.

**Log Entry Composition - Data, Component, or Resource Identity** - Every log and audit trail entry captured by a Company X computer or communication system must contain the identity or name of affected data, system component, or resources associated with the entry.

Log Analysis and Reporting

**Log Viewing** – To facilitate the analysis of log data, all event logs for Company X systems must be made available in a human-readable format.

**Log Reporting** – To facilitate the analysis of log data, Company X must implement tools necessary to report on the events found within event logs.

**Log Normalization** – To facilitate analysis and event detection, all Company X log data must be normalized to a consistent time and date format.

**Security Event Monitoring (SEM)** – Company X must employ security event monitoring software to facilitate the collection, storage and analysis of system audit logs.

**Host-Based Intrusion Detection** – Company X must employ host-based intrusion detection software on all critical information systems.

**Logging Network** – Log information transferred between logging hosts and servers must run over a separate network segment dedicated to log activity.

### **Management**

**Log Retention Period** - Every log and audit trail produced by a Company X computer or communication system must be retained for at least one year.

**Remotely-Mirrored Logs** - Every Company X production information system that is accessible by any external network must employ remotely mirrored system logs.

**User-Initiated Security Event Logs** - One or more logs tracing security relevant activities to specific users must be securely maintained for a reasonable period of time.

**Removal Of Logs From Internet-Accessible Computers** - If they are resident on Internet-accessible computers, system logs and application logs must be moved at least daily to other machines that are not directly Internet-accessible.

**System Log Rotation And Archival** - To prevent the overwriting of system logs or the expansion of these logs to the point where they consume all available disk space, a formal log rotation and archival storage process must be employed for all network periphery security systems and all multi-user production servers.

**Centralized Log Host Required** - Server system logs must be recorded on both the involved servers and also a central log host. These logs must be securely maintained for the time periods stated in server configuration standard issued by the Information Security Department.

**Log Restoration** - Process must be in place to be able to restore at least the last three months’ of any log or audit trail produced by a Company X computer or communication system for immediate analysis.

### Protection of Log Information

**System Log Integrity Check** - All Company X production information systems must employ cryptographic checksums to protect system logs.

**Limited Log Access** – Only system administrators with approved access will be allowed to access, modify or archive log data.

**Log Deactivation, Modification, Or Deletion** - Mechanisms to detect and record significant computer security events must be resistant to attempts to deactivate, modify, or delete the logging software and logs.

**System Log Protection** - All Company X production computer system logs must be protected with digital signatures and log entry sequence numbers.

**System Log Monitoring** – All Company X production computer system logs must also be automatically monitored for sudden decreases in size, failures of digital signatures, and gaps in log entry sequence.

**Systems Software Utility Usage** - Access to systems software utilities must be restricted to a small number of trusted and authorized users that are approved by the Information Technology Department.

### Log Storage and Maintenance

**System Log Rotation and Archival** - To prevent the overwriting of system logs or the expansion of these logs to the point where they consume all available disk space, a formal log rotation and archival storage process must be employed for all network periphery security systems and all multi-user production servers.

**Log Retention Period** - Every log and audit trail produced by a Company X computer or communication system must be retained for at least one year.

**Log Clearing** - System administrators must perform maintenance to purge or delete log entries older than 1 year on any system or event logs.

**Log Disposal** – All Company X system logs are considered confidential information and must be properly disposed of and destroyed.

### Clock Synchronization

**Clock Synchronization** - All multi-user computers connected to the Company X internal network must always have the current time accurately reflected in their internal clocks.

**Timeserver Technology** - The time setting on all Company X computer and communications system components must be kept current using a known, stable version of Network Time Protocol or similar technology.

**Timeserver Designation Limitation** - No more than two or three Company X internal servers must be designated as timeservers to receive time signals from multiple sources.

**External Time Update Designation** - Specific external hosts must be designated from which Company X timeservers accept Network Time Protocol time updates.

### Example Roles and Responsibilities

**System and network administrators** are responsible for configuring logging on individual systems and network devices, analyzing those logs periodically, reporting on the results of log management activities, and performing regular maintenance of the logs and logging software.

**Security administrators** are responsible for managing and monitoring the log management infrastructures, configuring logging on security devices (e.g., firewalls, network based intrusion detection systems, Antivirus servers), reporting on the results of log management activities and assisting others with configuring and logging and performing log analysis.

**Computer security incident response team (CIRT)** uses log data when handling and responding to specific incidents

**Application developers** must design or customize applications so that they perform logging in accordance with the logging requirements and recommendations

Information security officers oversee the log management infrastructures

**Chief information officer (CIO)** oversees the IT resources that generate, transmit, and store the logs.

**Internal and External Auditors** use log data when performing audits

**Software Procurement Team** - Individuals involved in software procurement should insist that all system purchased or developed can correspond to the corporate logging standards.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Audit Trail** - A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.

**Audit Log** - A record of transactions in an information system that provides verification of the activity of the system.

**Confidential Information (Sensitive Information)** - Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a third party under a non-disclosure agreement.

**Host-Based Intrusion Detection Systems (IDS)** – A host-based IDS monitors the characteristics of a single host and the events occurring within the host for suspicious activity.

**Log file integrity checking** - Integrity checking involves calculating a message digest for each file and storing the message digest securely to ensure that changes to archived logs are detected. A message digest is a digital signature that uniquely identifies data and has the property that changing a single bit in the data causes a completely different message digest to be generated.

**Log normalization** – Normalize is achieved when each log data field (for example, date-time field) is converted to a particular data representation and categorized consistently. One of the most common uses of normalization is storing dates and times in a single format.

**Log rotation** - Rotation is closing a log file and opening a new log file when the first file is considered to be complete. Log rotation is typically performed according to a schedule (e.g., hourly, daily, weekly) or when a log file reaches a certain size. The primary benefits of log rotation are preserving log entries and keeping the size of log files manageable.

**Log Parsing** – Parsing is extracting data from a log so that the parsed values can be used as input for another logging process. A simple example of parsing is reading a text-based log file that contains 10 comma-separated values per line and extracting the 10 values from each line.

Parsing is performed as part of many other logging functions, such as log conversion and log viewing.

**Log Archival** - Log archival is retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server. Logs often need to be preserved to meet legal or regulatory requirements.

**Partner** - Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**System Log** - A file that contains and stores events that are captured by operating system or application components. These events are often predetermined by the operating system itself. System log files may contain information about device changes, device drivers, system changes, events, operations and more.

**Timeserver** – A device that obtains the time of day for synchronizing PCs, servers, routers and switches on the local network. It picks up the time from the GPS satellites as well as NTP servers on the Internet.

**User** - A person, organization or entity that interacts with data for the purpose of performing an authorized task.

References

CPL: 15.01 Logging and Monitoring

ISO/IEC 27002: 12.4 Logging and monitoring

HIPAA: Audit Controls 164.312(b)

PCI: R10. Track and monitor access to networks and cardholder data

NIST: Audit and Accountability (AU)

NIST SP 800-92 Guide to Computer Security Log Management

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |