Computer and System Logging Policy

1. Overview

Computer logs are essential to the operational management of an organization. They provide a primary mechanism for automated tracking and reporting for review, audit, and compliance functions as well as a useful mechanism for tracking changes and troubleshooting.

2. Purpose

Frequent monitoring and logging components are required to effectively assess information system controls, operations, and general security. This policy provides a set of logging policies and procedures aimed to establish baseline components across the Thiel College Network.

3. Scope

This policy applies to all Thiel College staff that create, deploy, or support application and system software.

4. Policy

A. GENERAL

Access to Thiel College's network, systems and communications shall be logged and monitored to identify potential misuse of systems or information. Logging activities shall include regular monitoring of system access to prevent attempts at unauthorized access and confirm access control systems are effective. Log servers and documents shall be kept secure and only made available to personnel authorized by the Director of Information Systems. These logs shall be kept as long as necessary or required for functional use or appropriate state regulation or law.

Thiel College's information systems (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to:

- Ensure use is authorized
- Manage, administer, and troubleshoot systems
- Protect against unauthorized access
- Verify security procedures and access
- Verify system and operational security
- Comply with Thiel College policies and procedures

- Detect and prevent criminal or illegal activities

The system administrator shall implement automated audit trails for all critical systems and components. At a minimum, these logs shall be used to reconstruct the following events:

- Individual user accesses to systems and sensitive information
- All actions taken by any individual with administrative privileges
- Access to audit trails
- Invalid logical access attempts and failures
- 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 administrative privileges
- Initialization, stopping, or pausing of the audit logs
- Creation and deletion of system level objects

B. 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 to:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed (subject)
- Systems and objects involved
- When the activity was performed
- Status (such as success vs. failure), outcome, and/or result of the activity

Thiel College shall implement a suitable logging infrastructure and configure all critical devices, systems, and applications with logged audit trails. The system administrator shall ensure important events and audit trails are logged. File integrity

monitoring/change detection software shall review logs and issue alerts if the log data is altered.

C. ACTIVITIES TO BE LOGGED

Support staff shall be assigned to review and monitor the logs for systems under their control. Logs shall be reviewed on a regular and on-going basis. The frequency of review shall be determined according to the sensitivity of the information stored, the function of the system, and other system requirements as determined by the system administrator. Procedures should verify that logging is active and working properly to:

- Ensure events are properly classified
- Review logging for performance delays
- Ensure compliance related logging cannot be bypassed
- Verify access to log files is properly restricted
- Assist with investigations

Logs shall be created whenever the following activities are performed by a system, application, or user:

- Creating, reading, updating, or deleting confidential information, including confidential authentication information such as passwords
- Initiating or accepting a network connection
- Authenticating user access and security authorizations
- Granting, modifying, or revoking access rights to include new user or group additions, user privilege modifications, file or database object permissions, firewall rules, and user password changes
- Configuring systems, networks, or services for maintenance and security changes including installation of software patches and updates, or other installed software
- Changing statuses of application process startup, shutdown, and/or restart
- Application process aborts, failures, or abnormal conditions due to resource limits or thresholds (such as for CPU, memory, network bandwidth, disk space, or other key system resources), failure of network services, or hardware faults

- Detection of suspicious/malicious activity such as from an intrusion detection or prevention system, anti-virus, or anti-spyware system

D. SYSTEM LOG ELEMENTS

System events and activities that shall be monitored and logged are as follows:

- System administrator and system operator activities
- System start-ups and shut-downs
- Logging start-ups and shut-downs
- Backups and restorations/roll-backs
- Exceptions and security events
- Database commits and transactions
- Protection software and 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)

E. APPLICATION LOG ELEMENTS

Third party and custom application software logging requires more than just relying on server based system logs. Application logs help identify security incidents, establish baselines, provide information about problems and unusual conditions, assist with incident investigation, and help detect intrusions and errors. Application events and activities that shall 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 modifications)
- 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. adding and deleting users, changes to access privileges, use of administrative privileges, access by application administrators, and access to sensitive data)
- Legal compliance services (e.g. permissions to transfer information, terms of use, and parental consent)
- Security events or warnings

F. LOGGING ELEMENTS

Log entries can contain a number of elements based on the type and function of the audited system/process. Generally, automated audit trails shall include the following information:

- Host name, system component, or resource
- Date/Time Stamp
- Application ID (e.g. name and version)
- Initiating Process ID or event origination (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)

G. FORMATTING AND STORAGE

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

- Collecting Microsoft Windows Event Logs from servers by a centralized logging management system

- Storing logs in a documented format and sent via reliable network protocols to a centralized log management system

- Storing log entries in a SQL database that generates audit logs in compliance with the requirements of this policy

H. INFORMATION SECURITY ISSUES

Logs are one of the primary tools used by system administrators and management 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 and limit log security risks such as:

- Controls that limit the ability of administrators and those with operating system command line access to disable, damage, or circumvent access control and audit log mechanisms

- Protecting the contents of system logs from unauthorized access, modification, and/or deletion

- Limiting outside access to logging systems to extreme or emergency circumstances. Any emergency access should be authorized by the [Insert Appropriate Role] and use of tools bypassing security controls should be documented

- Limiting changes to the auditing policies to stop logging of an unauthorized activity. Log settings should be set to track and record user policy changes

I. ADMINISTRATIVE RESPONSIBILITIES

The system administrator shall be responsible for:

- Separating duties between operations and security monitoring
- 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
- Procedures ensure that the audit controls meet security requirements by recording and examining activity related to sensitive information
- Securing audit trails by limiting viewing 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

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Thiel College procedures. Examples of auditable controls include:

- On demand and historical log reviews of areas described in this policy
- Documented communications surrounding logging activities
- Incident response procedures

6. Enforcement

Staff or faculty members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all Thiel College staff, faculty and contractors using Thiel College information resources.