Audit Log Management Policy

1.0 Purpose
To identify the specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with the University's log management strategy.

2.0 Scope
This document applies to all servers, applications and network devices that handle, accept network connections, or make access control (authentication and authorization) decisions for access to sensitive Lawrence Technological University data.

3.0 Policy Statement
Information Technology Services shall implement an audit log management program that includes generating, transmitting, storing, analyzing, and disposing of computer log data. This program will:

- Audit logs recording user activities, exceptions (i.e., errors or failures), and information security events should be generated commensurate with the security requirements of the system being monitored.
- Audit logs should be retained for at least 120 days.
- Enterprise information systems must log system administrator activities, such as the use of privileged accounts (e.g., supervisor, administrator, or root).
- Audit logs should be periodically reviewed to detect security violations.
- Security event log data must be protected against unauthorized access and alteration.
- Clocks of systems being monitored should be synchronized regularly from an accurate time source.