Log Management Standard

Policy Title:
Log Management Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This document applies to all servers and network devices that handle, accept network connections, or make access control (authentication and authorization) decisions for Loyola Protected information, as defined within the Data Classification Policy. In addition, please note that this policy covers all IoT devices. Checking logs daily minimizes the amount of time and exposure of a potential breach. 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.

II. Definitions

Card Holder Data: is any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder data includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date or service code.

Sensitive Authentication Data: is the information on a card used for authentication at the time of a purchase. This includes data from the full magnetic strip, card security code (CSC, CVV2, CID, CAV2), and PIN and/or PIN block.

IDS: is a network security technology originally built for detecting vulnerability exploits against a target application or computer.

IPS: is a technology that keeps an eye on a network for any malicious activities attempting to exploit a known vulnerability.

DHCP: is a network protocol that is used to configure network devices to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration

information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

DNS: translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.2.44).

III. Policy

The University Information Security Office (UISO) will perform a daily review of security event logs as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. as is necessary to identify potential issues. Additionally, the UISO will monitor and analyze alerts and distribute to appropriate personnel.

The following events are reviewed at least daily:

- All security events
- Logs of all system components that store, process, or transmit Card Holder Data (CHD) and/or Sensitive Authentication Data (SAD)
- Logs of all critical system components
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)

Underlying requirements

All covered systems shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including from where or from which system the activity was performed?
- What the activity was performed on the covered system?
- When was the activity performed?
- With which program(s) was the activity was performed?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Activities to be logged

Logs shall be created whenever any of the following activities are requested to be performed by a covered system:

- Create, read, update, or delete Loyola Protected or Loyola Sensitive information, and authentication information such as passwords
- Initiate a network connection
- Accept a network connection

- User authentication and authorization for activities covered in #1 such as user login and logout
- Grant, modify, or revoke 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 service configuration changes, including installation of software patches and updates, or other installed software changes
- Application process startup, shutdown, or restart
- 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 Prevention System (IPS), anti-virus system, or other security systems.

Elements of the log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete, and accept network connection.
- Subsystems performing the action – examples include process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Before and after values when action involves updating a data element, if feasible.
- Date and time the action was performed, including relevant time-zone information if not in Universal Time. This date and time shall be synchronized using the University's NTP servers.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

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. All audit logs must be kept for one year, with three months available online.

Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

- Microsoft Windows Event Logs collected by a centralized log management system;
- Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system; and
- Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document.

Access to Log Files

All access to log files and audit trails shall be limited to a user's job-related need to know, as per the ITS Access Control Policy. Audit trails shall be protected from unauthorized modifications. All log information is transmitted, near real time to a SIEM for aggregation and analysis.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Log Management Standard at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- Data Classification Policy
- ITS Access Control Policy
- ITS Security Policy

Approval Authority:	ITESC	**Approval Date:**	June 7th, 2017
Review Authority:	Jim Pardonek	**Review Date:**	July 31st, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu