UNIVERSITY OF NEBRASKA AT OMAHA

Effective: 01-01-2009
Last Revised: 08-31-2016

Responsible University Administrator:
Chief Information Officer

Responsible University Office:
Information Security

Policy Contact:
Information Security • security@unomaha.edu

Audit Logging and Review

POLICY CONTENTS

Scope

This policy applies to all systems and university employees that are subjected to and must adhere to the Payment Card Industry Data Security Standards (PCI-DSS). Other systems and employees are advised to use this document as a best practice.

Policy Statement

Audit Logging and Review

Security auditing must be enabled on all university infrastructure components that support logging. The resulting logs must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, policies and standards at the university. Logs must be archived and reviewed for security irregularities.

Audit Settings

Operational staff must maintain a log of significant activities, listed below, on their systems including exceptions to normal processing. The audit logs should be set to record sufficient information for the logs to be reviewed through automated or manual processes. The audit logs should contain the following information as appropriate:

- Identification of the person or account making the log entry
- Origination of audit event
- Date and time of the log entry
- System errors and operator response

- All suspicious activity, which might be an indication of unauthorized usage or an attempt to compromise security

Significant Activities

Information systems at the university, provided they support these activities, must have auditing features configured to record security-related events at a minimum. The auditing features must log the following events:

- Failed authentication
- Successful authentication
- Failed access
- Privileged access usage
- Failed system shutdown
- Successful system shutdown
- Initialization of audit logs
- Creation/Deletion of system level objects

System administrators must configure auditing features to record audit events to a log file. The log file must be of sufficient size to retain data for at least thirty (30) days before it is copied. The log files must be copied to a secured directory for archival and backup to a centralized system. Access to log files must be restricted to authorized personnel only. A common source of clock time is to be used on systems throughout the organization whenever possible and practical. This aids log reviews in synchronizing and correlating activities that occurred on separate systems.

Log Alerting & Review

Systems deemed critical to mission operations, information security (e.g. firewalls, domain controllers, and critical database servers), and those that are subjected to specific regulatory and/or industry requirements (e.g. PCI or HIPAA) must be configured to provide near real-time alerting of security-related events. These alerting mechanisms may be native to the operating system/application or be provided by third-party software utilities. Alerts may also be reported by users. At a minimum, alerts should be communicated to system administrators via e-mail. Logs are also used in the event of an incident for both investigative and forensic purposes. All potential security violations should be reported as defined in the UNO Information Security Incident Response Policy.

Alerts must be reported and corrective action must be taken. Alerts reported by users regarding problems with information processing or communications systems are to be logged. There are clear rules for handling reported errors including:

- Review of alerts and problem logs to ensure that errors have been satisfactorily resolved
- Review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized

Audit logs for critical systems are reviewed on a periodic basis to ensure that the proper information is being captured. Where automated mechanisms are not in place to alert of security incidents, manual review of log files occurs on a periodic basis to determine whether any security-related events have occurred. The log reviews are conducted by an employee with a sufficient level on knowledge to determine whether a security related event has occurred.

Log Retention for PCI Systems

Audit logs are to be retained for at least one (1) year. In addition, three (3) months of logs are to be immediately available for analysis, either online or restored from backup.

Reason for Policy

Audit logging and review are essential in ensuring a diligent and proactive information security and systems environment. This policy outlines the requirements for audit logging and review with the intent of identifying user and system activity in order to reduce the risk of unauthorized access/ disclosure and availability of university information assets.

Related Information

UNO Digital Security Incident Response Policy

This policy covers the following sections of ISO 27001:

- 10.10.1 Audit logging
- 10.10.2 Monitoring system use
- 10.10.3 Protection of log information
- 10.10.4 Administrator and operator logs
- 10.10.5 Fault logging
- 10.10.6 Clock synchronization

This policy covers the following sections of PCI-DSS 3.2:

- 10.1 Implement audit trails to link all access to system components to each individual user.
- 10.2 Implement automated audit trails for all system components to reconstruct events.
- 10.3 Record at least the following audit trail entries for all system components for each event.
- 10.4 Using time-synchronization technology, synchronize all critical system clocks.
- 10.5 Secure audit trails so they cannot be altered.
- 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.
- 10.7 Retain audit trail history for at least 1 year, with a minimum of 3 months immediately available for analysis.

History

This policy is an update to the Audit Logging & Review Policy that was previously updated in 2009.
