Purpose and Benefits

Log generation and management is necessary to protect the confidentiality, integrity, and availability of our Information Resources and the data contained therein. Event logging supports the continued delivery of operations and improves the security and resilience of critical Information Resources by enabling visibility.

Developing and implementing Enterprise-wide logging procedures improves UNT System chances of detecting malicious behavior on our Information Resources and enforces a consistent method of logging across our environment. The purpose of this standard is to establish requirements for system logging across UNT System Enterprise.

Authority and Requirements

Audit Logging and Accountability section of the UNT System Information Security Handbook (Page 47-48). The Audit Logging and Accountability requirements of the UNT System Information Security Handbook satisfy the control requirements of AU – Accountability, Audit, and Risk Management in the Texas Department of Information Resources Security Controls Standards Catalog.

Definitions

Event. “Event” means something that occurs within an Information Resource, including networks.

Information Security Program. “Information Security Program” means the policies, Information Security Handbook, control catalog, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions. The Information Security Program shall comply with applicable federal and state laws related to information resources and information security, including but not limited to 1 Texas Administrative Code §202 and the State of Texas Department of Information Resources Security Controls Standards Catalog.

Information Resources. “Information Resources” means the procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

Log. “Log” means a record of the events occurring within an Information Resource, including networks.

Log Reduction. “Log Reduction” means removing unneeded entries from a log to create a new log that is smaller.

Log Retention. “Log Retention” means archiving logs on a regular basis as part of standard operational activities.

Mission Critical. “Mission Critical” means an Enterprise information resource that the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of the UNT System Enterprise.

General Implementation

Information Resources shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of UNT System proprietary and confidential information.

System Administrators must maintain appropriate audit trails to provide accountability for updates to Information Resources for all changes to automated security or access rules. A sufficiently complete history of transactions must be maintained to permit an audit of Information Resources by logging and tracing the activities of individuals.

Normalizing Clocks and Timestamps

Information Resources participating in log generation and management should normalize their clocks using a common network time protocol where available and should ensure logs contain timestamps that include millisecond granularity.

Information Resources Required to Log Events

The following Information Resources are required to log events:

- Information Resources deemed mission critical,
- Information Resources that are dependencies of mission critical systems,
- Information Resources that transmit, process or store mission critical or confidential information,
- Information Resources subject to legal, regulatory, or contractual obligations,
- Information Resources that can affect the security of any of the above categories,
- Information Resources that have previously experienced major security incidents, and
- Information Resources that are internet facing.

System Administrators of Information Resources deemed mission critical must work with UNT System Security Operations to ensure logs are centralized, including but not limited to, Microsoft Authenticator, Virtual Private Networks, and Enterprise Information Systems.

Categories and Events

Events to be logged vary on log source and log source configuration. System Administrators should identify the types of events that an Information Resource is capable of logging, to document individual accountability for actions on the Information Resource. Categories and suggested event types are as follows:

Categories	Events
Hardware	• Authentication Attempts: Successful and failed login attempts, including user IDs and IP addresses. • Access Control Changes: Modifications to user permissions and roles. • User Activity: Actions performed by users, such as file access, modifications, and deletions. • Startups and Shutdowns: Logs of when devices are powered on or off. • Hardware failures, disk errors, and other critical system issues. • Resource Usage: CPU, memory, and disk usage statistics. • Configuration Changes: Changes to system settings, and security policies • Security Incidents: Detection of malware, unauthorized access attempts, and other security breaches. • Service Status: Availability and performance of critical services.
Operating Systems and Applications	• Authentication Attempts: Successful and failed login attempts, including user IDs and IP addresses. • Access Control Changes: Modifications to user permissions and roles. • User Activity: Actions performed by users, such as file access, modifications, and deletions. • Performance Metrics: Application performance data, including response times and throughput. • Errors and exceptions generated by applications. • Changes to settings, security policies, and configurations. • Security Incidents: Detection of malware, unauthorized access attempts, and other security breaches. • Service Status: Availability and performance of critical services. • Transaction Logs: Records of transactions processed by applications.
Network	• Network Traffic: Logs of incoming and outgoing network traffic, including source and destination IP addresses. • Firewall Activity: Changes to firewall rules and detected intrusions. • VPN Connections: Establishment and termination of VPN sessions.

Audit Information Details

Audit information of ingested logs should contain the following detail fields:

Minimum Required	Additional as Available

▪ Timestamp (UTC -5) ▪ Source and destination IP address ▪ Protocol method ▪ Status code ▪ Request details	▪ Device Identifier (MAC or unique identifier) ▪ Response Time ▪ EUID ▪ Headers ▪ Command or action taken ▪ Event Identifier

Log Format

Logs should use standardized formats, or a log parsing guide should be maintained for any parsing needs.

Log Storage

Logs must be stored in a centralized log management system to facilitate analysis and correlation. Centralized log management systems must be separate from the Information Resource generating the logs, ensuring the integrity of the log information. Centralized log management systems must follow logging and monitoring standards contained herein.

Log Retention

Information Resource logs must be retained to comply with regulatory requirements and support forensic investigations. Information Resource log retention should be no less than 30 days and should comply with the institutional record retention policy.

Information Resources subject to elevated security requirements should follow log retention requirements in accordance with those requirements (e.g. CJIS and NIST 800-171 Rev 2).

Log Review and Reporting

Regular log reviews ensure a secure and efficient information technology environment. System Administrators should review Information Resource logs for the purposes of security monitoring, performance analysis, troubleshooting, audit trails, and ensuring compliance.

Any anomalous behavior discovered in logs should immediately be reported to the Information Resource System Administrator. System Administrators must report anomalous log activities immediately to UNT System Security Operations.

Protecting Audit Logs

Logs shall be protected from unauthorized access, modification, and deletion in accordance with the UNT System Information Security Program. Encryption that complies with the UNT System Cryptographic Standard must be used to store log data at rest.

Log Reduction

System Administrators should implement log reduction to comply with security requirements, as applicable. Log reduction may be performed through the implementation of log filtering to reduce the volume of logs by excluding non-essential information while retaining critical security events. The use of log aggregation techniques may be used to consolidate logs from multiple sources, reducing redundancy and improving analysis efficiency. System Administrators may apply compression algorithms to reduce the storage footprint of log data without losing essential information.

Log Transmission

Logs must be transmitted securely using encryption protocols that meet the UNT System Cryptographic Standard to protect data in transit. Implement real-time log transmission to ensure timely detection and response to security incidents.

Audit Logging Process Failures

When alerted to a log processing failure the System Administrator must be immediately notified to remediate the failure and restore logging processes.

Exceptions and Compensating Controls

Exceptions to Information Security policies and this standard may be approved by the Associate Vice Chancellor and Chief Information Security Officer or their designee when accompanied with sufficient justification and compensating controls, in accordance with the UNT System Information Security Program.

The Associate Vice Chancellor and Chief Information Security Officer may revoke an exception at any time.

References and Notes

DIR Security Controls Standards Catalog
UNT System Information Security Regulation 06.1000
UNT System Information Security Handbook
UNT System Access Control Standard
UNT System Cryptographic Control Standard
NIST Special Publication 800-92, Guide to Computer Security Log Management

Approvals and Revision History

	Name	Title	Date
Authored By:	Paula Mears	Director of Security Operations	6/24/2024
Approved By:	Rich Anderson	Chief Information Security Officer	10/22/2025

Date	Approved By	Version	Notes
7/3/2024	Rich Anderson	1.0	New Logging Management Standard
10/22/2025	Rich Anderson	2.0	Enhanced Logging Management Standards