UNT SYSTEM™
Information Technology

Logging Management Standard

Overview and General Requirements

Log generation and management is necessary to protect the confidentiality, integrity, and availability of our systems and the data contained therein.

Information systems participating in log generation and management should normalize their clocks using a common network time protocol where available. Log retention should be no less than 30 days.

Systems Required to Log Events

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

Log Categories

- Operating Systems
  - System Events – Operational actions performed by OS components
    - Shutting down
    - Starting or stopping a service
    - Network events
  - Audit Records
    - Authentication events – successes and failures
    - File access
    - Security policy changes
    - Account changes
    - Use of privileges

- Applications
  - Client requests and server responses
  - Account information
  - Usage information
  - Significant operational actions
  - Major application configuration changes

- Network Equipment
  - Routers

- Firewalls
- Web proxy servers
- Network gateways

- Security Products
  - Endpoint protection products
    - Vulnerability assessment information
    - Penetration test reports

Log Details

Specific log details vary depending on the log source and configuration. System custodians should identify the types of events that a system is capable of logging to establish individual accountability for any action on that system that potentially cause access to, generation or modification of, or affect the release of confidential information. Below are the minimum recommended fields to capture.

- Timestamp
- Source and destination IP address
- Protocol method
- Status code
- Request details

Centralized Log Storage

Logs are required to be stored in a centralized location separate from the system generating the log information. Capturing and storing logs in a separate location from the system upon generation ensures the integrity of the logged information.

Log Protection

Logs should be encrypted in transit and properly secured in storage to protect the confidentiality and integrity of the logs.

Logs are Category I Confidential Information and should be protected according to the measures and controls described in the UNT System Information Security Handbook and the DIR Security Controls Catalog.

Reference

NIST Special Publication 800-92 Guide to Computer Security Log Management

UNT System Information Security Handbook Section 12.7 Monitoring, Section 8 Asset Management

DIR Security Control Standards Catalog 2.0 Section AU – Accountability, Audit, and Risk Management

Document Version Log

Version	Date	Description
1.0	6/7/2022	Initial Document Version
1.1	9/27/2022	Document approved
1.2	1/25/2023	Document revised to include DIR SCSC AU-2 requirements, changed from Best Practices to a Standards document
1.3	3/31/2023	Provided clarification on Centralized Log Storage and Log Protection. Modified for formatting.