University System of New Hampshire

Security Monitoring and Log Management Standard

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: ET&S Cybersecurity GRC
Approved Distribution: Public
Status: In Force

1. PURPOSE

Enterprise Technology & Services (ET&S) is charged by the University System of New Hampshire (USNH) to protect the integrity, confidentiality, and availability of systems and information. This standard establishes consistency in creating and managing information systems activity and logs across the university system. Ensuring system logs are available and monitored consistently aids the identification of security events and may help prevent security incidents or minimize the potential impact of incidents.

2. SCOPE

This standard applies to all USNH IT assets. This standard applies to all USNH System institutions.

3. AUDIENCE

All USNH community members who access USNH information technology resources should be familiar with this Standard.

4. STANDARD

University System of New Hampshire

4.1 Establish and Maintain Event Monitoring and Log Management Process

USNH ET&S shall establish and maintain a process to capture key security events associated with information technology resources. Two types of logs are generally treated and often configured independently: system logs and audit logs. System logs record information that may signal system problems (for example, database read errors, rollbacks). All USNH technology assets shall have system logging enabled.

Audit Logs record security-related events used to reestablish a series of events and potentially contain sensitive, protected, and/or restricted information. All USNH employees handling audit logs shall comply with all federal, state, and institutional data protection regulations and policies.

Audit logging and alerts are required to be enabled on the following USNH assets:

- Any system accepting network connections including, but not limited to remote access systems (Virtual Private Networks), Firewalls, proxies, Intrusion Detection Management (IDM) systems, and security Information and event management (SIEM) systems
- Any system involved in access control
- Any system handling sensitive, protected, or restricted information per the USNH Information Classification Policy

The systems mentioned above shall be referred to as critical systems in the remainder of this standard. Audit logging and event monitoring capabilities for USNH critical systems shall be activated at all times, with logs sent and stored to centralized logging servers. ET&S shall ensure all logging destinations have and maintain adequate storage to comply with this standard. Responsible parties shall review the audit logs weekly at a minimum.

All USNH systems shall set each logging host to the correct time zone, and clocks are synced to USNH time servers or a trusted external time source.

4.2 Required Audit Log Information

USNH institutions and entities shall ensure that, at a minimum, the following system events are logged centrally and monitored for critical systems:

- All authorized user access to protected information, including:
    - User ID
    - Date and time of key events
    - Types of events
    - Files accessed when feasible.
    - Program/utilities when possible.
    - Network addresses and protocols

- All operations and actions taken by any individual with elevated privileges:
    - System startup and stop
    - System clock time change
    - I/O device attachment/detachment
    - Modification/flushing of local log files
    - DNS queries
    - URL requests
    - Command-line implementations including audit logs from PowerShell, BASH, and remote administrative terminals

- Unauthorized access attempts:
    - Failed or rejected user actions
    - Failed actions involving restricted information or system components
    - Access violation notifications for network gateways and firewalls
    - Alerts from proprietary intrusion detection systems

- System alerts or failures:
    - Console alerts or messages
    - Network management alarms
    - Events/alarms from identity and access control systems
    - Hardware/Software errors
    - Log storage capacity being reached or exceeded
    - Access control alarms

- Changes to system configuration and controls:
    - Stopping or pausing the audit logs
    - Changes to critical system configuration
    - Activation and deactivation of system protections (e.g., antivirus, intrusion detection, logging mechanism)
    - Security log processing or capturing failures
    - Database rights changes

- Changes to identification and authentication mechanisms, including but not limited to:
    - New account creation and privilege elevation
    - Deletions, additions, or changes to accounts with administrative or root privileges.

4.3 Log Handling and Retention

Audit log retention may be dictated by regulations that govern the stored data. All USNH log collection, storage, and retention shall comply with the USNH Information Classification Policy and federal regulations or laws governing the applicable data.

Regulatory Log Retention Requirements (not exhaustive)

- The Health Insurance Portability and Accountability (HIPAA): 7 years
- Payment Card Industry Data Security Standards (PCI DSS): 1 year
- Federal Information Security Management Act (FISMA): 3 years
- Gramm-Leach-Bliley Act (GLBA) – 6 years

USNH Data Classification Log Minimum Retention Requirements

- Tier 4 - Restricted Information: 180 days
- Tier 3 – Protected Information: 180 days
- Tier 2 – Sensitive Information: 90 days

Logs related to data not governed by any other consideration shall be retained for 90 days.

4.3.1 Log Protection

USNH ET&S shall protect logs from unauthorized access per legal, regulatory, and contractual obligations. Such actions include but are not limited to:

- Logs gathered from critical systems shall be automatically transferred to the USNH centralized log management data infrastructure or transferred to a centralized log service within three business days.

- ET&S must approve log access for individuals, or third parties not preauthorized to access logs.

- Implement controls to safeguard and protect logs and limit read access of audit trails to those with job-related needs.

- Use encryption or other approved forms of integrity protection for information in accordance with the USNH Information Security Classification Standard and/or regulatory requirements.

- Any interruption or failure of the logging process must be reported to the ET&S Cybersecurity Operations team. The report shall detail the cause, expected duration, expected remediation timeline, and classification of information impacted.

4.4 Log Review and Reporting

ET&S may review logs to detect and investigate anomalous events, analyze and/or troubleshoot systems and generate reports and/or metrics as well facilitate risk-based decision making.

Reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat should be done at a minimum weekly or more frequent basis.

5. ENFORCEMENT

Intentional or knowing violations of this standard may constitute misconduct. Accordingly, employees are subject to disciplinary action, up to and including suspension without pay and dismissal, in accordance with the pertinent employment policies for Staff and Faculty.

University System of New Hampshire

6. CONTACT INFORMATION

For USNH community members: Questions about this standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, & Compliance (GRC) via this Support Form.

Cybersecurity GRC will handle exception requests in accordance with the USNH Cybersecurity Exceptions Standard.

A community member may submit other requests here: Submit an IT Question.

7. DOCUMENT HISTORY

Effective Date: February 24, 2022
Drafted: USNH Tomi Gibson, ET&S Cybersecurity GRC, February 2022 v01
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, February 23, 2022
Revision History: Revised by Kelly Sweeney, ET&S Cybersecurity GRC, June 2023
Approved by: Thomas Nudd, Chief Information Security Officer, February 23, 2022