Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-04: Audit and Accountability Standard

Standard Contents

1. Purpose

The purpose of the Audit and Accountability Standard is to ensure that all the University's applicable systems, information, and data can support audit requirements, establish accountability for all users' actions, and provide the capability to identify and alert appropriate applicable parties of security, integrity, or availability issues. This includes ensuring that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. Additionally, this policy is meant to establish the processes to correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. The policy outlines the methods and requirements pertaining to audit logging, alerting, and monitoring procedures performed.

2. Scope

This Standard shall apply to all the University of Nebraska's ("University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this policy applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this Standard to indicate audit logging definitions, performance, detection and protection, and review. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer (CISO) as defined in **ITS Policy Exception Standard**. The following subsections outline the Audit and Accountability Standard.

4. Information Security Audit and Accountability

4.1 Audit Log Requirements

4.1.1 Event Logging

All production and critical systems, including operating systems, applications, security appliances, and networking devices within the University's environments must have audit logging enabled to audit for events that could adversely affect the confidentiality, integrity, or availability of University systems, and data, in alignment with established configuration standards and vendor hardening guidance. At a minimum, audit logging must be enabled to capture the following activities. Center for Internet Security (CIS) Benchmarks provides a comprehensive list of audit logging per technology/vendor:

- User access to systems and networks
- Actions taken by any individual or service with root/administrator privileges
- User access audit trails
- Invalid logon attempts
- Use of and changes to identification and authentication mechanisms (such as creation of new accounts, elevation of privileges, all changes to administrative or root privileges)
- Initialization, stopping, or pausing of audit logs
- Creation and deletion of system-level objects
- System start-ups and shutdowns
- All incoming and outgoing network activity, including but not limited to router and firewall network flow records, port scanning attempts, NAT gateways, and network access

4.1.2 Minimum Log Elements
All University logs must record sufficient information to establish what type of event occurred, the date/time of occurrence, location of occurrence, source of the event, outcome, and the identity of the user/subject associated with the event. Specifically, logs must record the following, at a minimum:

- User or system service identification
- Date/time of the event
- Affected system, information, data, or resource
- Origination and destination(s) of the event(s)

Privileged commands issued by system administrators must, where technically feasible, be traceable to specific individuals, even when using a shared administrator account.

4.1.3 Alerts on Audit Log Forwarding and Processing Failures
Monitoring must be configured to alert appropriate administrative personnel in the event of an audit log processing failure, which could include hardware failures, audit log storage limits, or software errors.

4.2 Audit Log Time Synchronization

4.2.1 Time Synchronization
All University systems must synchronize system time to an ITS approved network time protocol (NTP) service and must protect time configurations from unauthorized access or modification.

In cases where Network Time Protocol (NTP) or similar technologies cannot be used for time synchronization, local system time must be reviewed and adjusted accordingly for all systems at a minimum frequency of twice per year. All changes to time settings on critical systems must be logged, monitored, and reviewed.

4.3 Audit Log Protection and Retention

4.3.1 Protection of Logs
All University audit logs must be protected so they cannot be altered. Protection shall be provided with digital signatures and log entry sequence numbers and must also be automatically monitored for sudden decreases in size, failures of digital signatures, and gaps in log entry sequence. Additional measures that can be applied towards log protection are as follows:

- Protection of audit log files from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.
- Replication or transfer of audit log files to a centralized and isolated log server or media.
- Implementation of file integrity monitoring or change detection software.

4.3.2 Access to Logs
Access to view audit logs and Security Information and Event Management (SIEM) tools must be limited to authorized personnel with a readily demonstrable need for such access to perform their regular duties such as ITS personnel. Approval by the Chief Information Security Officer must be documented prior granting user access to the SIEM tool. Generation of audit reports and access to the audit logs must be on-demand or with reasonable effort. All others seeking access to these logs must first obtain approval from the Chief Information Security Officer.

Standard and administrative access to SIEM, log analysis and correlation systems (such as Splunk) is to be reviewed on an annual basis by the respective system / business owner.

4.3.3 Audit Log Retention

Audit logs must be retained in accordance with organizational data retention schedules to ensure the availability of audit logs for incident response and forensic investigation purposes.

Standard log archival periods (hot, warm and cold), retention periods and a verification process for all archival periods that require the logs to be re-ingested.

All logs shall be kept for a minimum of thirty (30) days, unless a longer time period is required per applicable laws or regulations. Logs related to credit card data per the Payment Card Industry Data Security Standard (PCI DSS) should be retained for at least one (1) year. Logs related to personal health information per the Health Information Portability and Accountability Act (HIPAA) should be stored for at least six (6) years.

After logs have met their retention requirement, they must be securely deleted.

4.4 Audit Log Protection and Review

4.4.1 Log Correlation and Analysis

All security event logs, as detailed in section 4.1 of this standard, must be sent to a secure, centralized repository for analysis, such as a Security Information and Event Management tool (SIEM). Rulesets must be established to continuously correlate log data and monitor events against organizationally defined threat scenarios and potential indicators of malicious activity.

When alerting is triggered, it is the responsibility of a Security Analyst to review logs for potential nefarious activity. All security events detected and alerted on should copy the ITS Security Services team.

Alerts in the SIEM tool should be configured based on risks identified during the annual IT Risk Assessment. Alerts should be based on indicators of compromise related to those top risks.

Business units who have experienced a security breach in the last year shall be monitored for a minimum of one year.

4.4.2 Audit Log Record Reduction

As a method of supporting the Audit log review requirements, Audit reduction and reporting generation capabilities must be established to summarize logging into meaningful metrics suitable for review and reporting.

4.5 Log System Maintenance

4.5.1 SIEM Maintenance

ITS Security must formalize the version requirements for the SIEM tool and any other log correlation and analysis tools. Systems should be updated as needed to current versions.

5. Standards and Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published