CHRISTOPHER NEWPORT

UNIVERSITY

Security Monitoring and Logging Standard

VERSION 1.5

June 2023
Department: Information Security

Proprietary Statement

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
August 2019	1.0	Initial Plan	Wendy Murray
November 2019	1.1	Updated Log Retention Requirement	Wendy Corrice
February 2020	1.2	Corrected Log Retention Requirement	Wendy Corrice
April 2021	1.2	Annual Review	Wendy Corrice
June 2022	1.3	Annual Review	Wendy Corrice
February 2023	1.4	Content revisions to align with VITA SEC501, updates and reviewed	Wendy Wilde
June 2023	1.5	Annual Review	Wendy Wilde

TABLE OF CONTENTS

INTRODUCTION

Logging is an essential information security control that is used to identify, respond, and prevent operational problems, security incidents, policy violations, fraudulent activity and optimize performance. The purpose of this standard is to identify the responsibilities for security monitoring and logging of Information Technology systems and define logging requirements. This standard and accompanying procedures establish the minimum requirements for IT Security Monitoring and Logging, intended to meet the control requirements outlined in VITA's SEC-501, Section 8.3 Audit and Accountability Family Controls AU-1 through AU-11.

SCOPE

This standard applies to any university-owned IT resource or service that stores, processes, or transmits data classified as restricted to include network infrastructure. Additionally, this includes any IT resources or services identified by the Information Security Officer as important to security operations.

ROLES AND RESPONSIBILITIES

This section summarizes the roles and responsibilities as described in the standard section.

Role	**Responsibilities**
System Owner	The CNU business manager with overall responsibility for system compliance, operation and management.
Data Owner	Determines based on system risk assessment and business needs that the IT system is capable of auditing and a minimum the following events: ● Authentication attempts ● Authenticated individuals ● Access time ● Source of access ● Duration of access and ● Actions executed
Information Security Officer and Information Security Analyst	Responsible for monitoring and reviewing security event logs, correlating information with other automated tools, identifying suspicious activities and reviewing alert notifications
System Administrators	Responsible for server operating system logging configuration and monitoring
Database Analysts	Responsible for database logging, monitoring the availability and performance of database and for providing corrective actions and/or alert notifications

STANDARDS STATEMENT

In accordance with VITA SEC501 Controls AU-1 through AU-11, Information Security Officer (ISO) and/or designee is responsible for the oversight of security monitoring and logging for university-owned Information Technology resources.

UNDERLYING REQUIREMENTS

Systems that handle restricted data, accept network connections or perform authentication and authorization shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity?
3. Where on or from what system the activity was performed?
4. When was the activity performed?
5. What was the status of the activity performed (success or failure)?

AUDITABLE EVENTS

1. All in-scope systems must, at a minimum, be capable of and configured to:
    a. Produce audit logs with necessary event information, and
    b. Have the ability to send audit log data to the log correlation engine or alternate storage location
2. Network devices such as firewalls or routers must be configured to log security data as well as errors.
3. Web services and database application services must maintain logs of all security, application and event related information.
4. Events should be logged in real time to the fullest extent possible, stored locally and forwarded to the log correlation engine or alternate storage location.

CONTENT OF AUDIT RECORDS

1. The System Administrator(s) will configure the system such that audit records contain sufficient information to, at a minimum:
    a. Establish what type of event occurred (i.e., event id)
    b. When (date and time) the event occurred (i.e., time stamp)
    c. Where the event occurred (i.e., destination IP address)
    d. The source of the event (i.e. source IP address)
    e. The outcome (success or failure) of the event
    f. The identity of any user/subject associated with the event (i.e, user id/process id) and
    g. File name(s) involved and access control rule if applicable

2. The System Administrator(s) will configure the system to log additional data, commensurate with sensitivity and risk determined by the Information Security Officer and/or data owner or system owner.

3. Information Security will centrally manage the content of audit records generated by in-scope systems, including, but not limited to firewalls, database servers and authentication servers.

AUDIT STORAGE CAPACITY

1. The System Administrator(s) will ensure audit storage capacity is allocated in accordance with system configuration such that the capacity is not exceeded.

RESPONSE TO AUDIT PROCESSING FAILURES

1. System Administrator(s) will configure system alerts in the event of system failures
2. Identified events that are considered a potential security event will be responded to as outlined in the Security Incident Response Plan.

AUDIT REVIEW, ANALYSIS AND REPORTING

1. The System Administrator(s) and/or Information Security will review and analyze information system audit records at least every 30-days for indications of inappropriate or unusual activity, and report any suspicious findings to the Data Owner.

2. The System Administrator and/or Information Security will adjust the level of audit review, analysis and reporting within the information system when there is a reported change in risk to operations, assets, individuals, or based on law enforcement information, threat intelligence or other credible sources of information.

3. If the system is classified as *restricted,* audit review, analysis and reporting processes must be integrated to support organizational processes for investigation and response to suspicious activities. The integrated approach correlates records from across different sources to gain situational awareness. Further integration of audit records with analysis of vulnerability scanning information, performance data and network monitoring information should be used to enhance the ability to identify inappropriate or unusual activity.

4. The information Security Team is responsible for monitoring of the infrastructure and log files on a continuous basis and documenting the activity.

TIME STAMPS

1. The system must be configured to generate timestamps to include both date and time. The time may be expressed in Coordinated Universal Time (UTC), Greenwich Mean Time (GMT), or local time with an offset from UTC.

PROTECTION OF AUDIT INFORMATION

1. Audit records, audit settings and audit reports must be protected from unauthorized access, modification and deletion.

2. Access to audit information must be restricted to the System Owner and authorized personnel to perform IT Security audits and/or investigate security incidents.
3. Regular backup and archival processes must be in place for audit files in order to protect historical log data and collect new log data processed by the log correlation engine.
4. The log correlation engine (LCE) must be protected as it will contain sensitive data pertaining to restricted systems.

AUDIT RECORD RETENTION

1. Information Technology Services will retain audit records for a minimum of 180-days in accordance with the Library of Virginia GS-113 requirements and to support for after-the-fact investigations of security incidents.

ASSOCIATED PROCEDURE

1. ITS System Logging Guidelines & Procedures

EXCEPTIONS

Exceptions to this standard will be handled on a case by case basis and approval of the Information Security Officer.

REFERENCES

VITA ITRM Information Security Standard (SEC501)

ITS System Logging Guidelines & Procedures

ITS Security Incident Response Plan

REVIEW

Next Review Date: June 2024