LOGGING AND MONITORING STANDARD

Contents

TEMPLATE information (DELETE BEFORE USING)

This template is provided as an example of a policy or procedure that is based on the NIST 800-171 standards. It should be used as a reference point to create your own policy. It is important to note that no policy or procedure is “one-size fits all” and this document will require modification before use.

Authority

State Administrative Manual (SAM) 5300.

State Administrative Manual (SAM) 5335: Information Security Monitoring

State Administrative Manual (SAM) 5335.1: Continuous Monitoring

State Administrative Manual (SAM) 5335.2: Auditable Events

Statewide Information Management Manual (SIMM) 5305-A: Information Security Management Program Standard

NIST 800-171r2: Protecting Controlled Unclassified Information (CUI) in Non-Federal Information Systems

NIST SP.800-61r2: Computer Security Incident Handling Guide

NIST Cybersecurity Framework

Purpose

The purpose of the Audit and Activity Review Standard is to document the requirement to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Definitions and Terms

Audit Controls: Technical mechanisms that track and record computer activities.

Audit Trail: A chronological set of logs and records used to provide evidence of a system's performance or personnel activity that took place on the system, used to detect misconfigurations, and identify intruders.

Scope

This policy applies to [COLLEGE] employees, contractors, subcontractors, vendors, consultants, advisors, and other personnel who have access to [COLLEGE] information assets without regard to data ownership.

Exceptions

No exceptions for this policy are currently in place.

[COLLEGE] reserves the right to amend, revoke or terminate this policy in part or in its entirety, as it may deem necessary from time to time in accordance with applicable law.

Policy Statement

[COLLEGE] is committed to conducting business in compliance with all applicable laws, regulations and [COLLEGE] policies. [COLLEGE] has adopted this standard to set forth the internal audit process for protecting [COLLEGE] data.

To ensure data security, [COLLEGE] will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain sensitive [COLLEGE] data. [COLLEGE] will clearly identify all critical systems that process sensitive information. [COLLEGE] will implement security standards to regularly review the records of information system activity on all such critical systems that process sensitive information.

[COLLEGE] will monitor the physical environment and the network to identify potential activity that could indicate a potential security incident. Monitoring for unauthorized personnel, unauthorized remote access, connections, devices, and software will be performed.

Responsibilities

The Information Technology leader will clearly identify:

- The systems that must be reviewed
- The information on these systems that must be reviewed
- The types of access reports that are to be generated
- The security incident tracking reports that are to be generated to analyze security violations
- The individual(s) responsible for reviewing all logs and reports

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Information Technology will be responsible for ensuring that all required logs are enabled as noted in the Audit Logs, Event Logs, and Log Requirements sections below.

Audit Logs

Audit logs will be enabled to provide a chronological series of logged computer events that relate to an operating system, an application, or user activities. These events may then be used to review user or system activities in the event of an incident or reviewed on a regular basis as part of regular audits.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include, where possible, items such as:

- User IDs
- Dates and times of log-on and log-off
- Terminal identity, IP address and/or location, if possible
- Records of successful and rejected system access attempts

Event Logs

Events shall be logged with the ability to associate recorded events to individual users. Logs shall contain enough information to reconstruct the following activities:

- User access to any sensitive data
- Administrative access to any system
- All authentication attempts, (pass and/or fail)
- Creation or deletion of system level objects
- Configuration changes
- Modifications to any user accounts, including, but not limited to, creation, alteration, or escalation of privileges
- Access and changes to root or kernel system files
- Access and changes to log files including stopping or pausing of the logs
- Additionally, logs must contain the following fields, where possible:
    - Date & Time
    - Type of event
    - Origination
    - Identity of affected data, system, and/or resource

Log Requirements

The following requirements must be met for the access and storage of all event logs:

- Logs must not be stored on the same system from which they originate and must be written to a separate robust system that has its own specific security parameters
- Limit access to logs to approved and authorized personnel
- Logs records must have time and date stamps
- File integrity monitoring software shall be installed to monitor all access and changes to log files
- Safeguards must be deployed to protect against unauthorized changes and operational problems including:
    - Disabling of the audit log
    - Altering the message types that are recorded
    - Editing or deleting log files
- Logs shall be retained for at least 1 year with at least 3 months available immediately and sufficient capacity will be maintained to ensure that logs are retained as required
- Audits must be conducted to verify the viability of logs and their security
- Logs must be reviewed daily, and it is recommended to use automated review software, such as a SIEM or SOAR solution, for this purpose
    - Appropriate triggers and alerts must be incorporated into any such automated review software used, such triggers and alerts must be tested regularly

- A documented standard shall be in place to respond to any alerts generated by log review or file integrity monitoring

Questions

Questions regarding the information in this Policy should be directed to [COLLEGE IT or SECURITY GROUP].

Relevant Standards

Area	Reference
NIST CSF	PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-7
NIST 800-53	AC-17 (1), AC-19, AU-1, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-11, AU-12
NIST 800-171	3.1.12, 3.3.1, 3.3.2, 3.3.8, 3.4.9, 3.10.2, 3.10.3, 3.14.6, 3.14.7
SIMM	Information Security Management Program Standard 5305-A
SIMM	Incident Reporting and Response Instructions 5340-A

NIST CSF Function & Category	
DETECT	Anomalies and Events (DE.AE)
	Security Continuous Monitoring (DE.CM)
	Detection Processes (DE.DP)

Appendix A – Sample RACI Matrix

RACI Matrices can be a useful tool to clearly assign roles in a logging and monitoring environment. The following roles are defined as follows:

- **(R)esponsible –** The one who completes the task.
- **(A)ccountable –** The one ultimately answerable for the correct and thorough completion of the deliverable or task. Delegates to the Responsible.
- **(C)consulted –** Subject Matter Experts whose opinions are sought. Two-way communication.
- **(I)nformed –** Those who are kept up to date often at conclusion. One-way communication.

Activity	Service Desk	Service Desk Manager	Network Engineer	CISO	Management
Receive / Review Events	R	A			
Escalate Events	R	A	I		
Investigate Potential Incidents	I	R	C	A	
Manage Logging / Monitoring Infrastructure		C	R	A	
Declare Cybersecurity Incident	I	I	C	R	A

R – Responsible / A – Accountable / C – Consulted / I – Informed