Security Logging and Monitoring Standard

From the Office of the Chief Information Officer, State of Minnesota

Version: 1.9
Effective Date: 1/1/2016
Revised: 12/31/2024
Approved: John Israel, State of MN Chief Information Security Officer **Date:** 2/27/2025

Standard Statement

Detective and preventive information security monitoring controls must be in place to support the confidentiality, availability, and integrity of State data and systems.

Employees must abide by the terms of this standard. Employees who violate this standard may be subject to discipline, up to and including discharge.

Table 1. Security Logging and Monitoring Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
1	Logging	Implement automated logging on all systems to reconstruct the following events: • All actions taken by accounts with root or administrative privileges. (All system administrator commands while logged on as system administrator) • Access to all log data. • All log-in attempts (successful and unsuccessful). • All system log offs. • Use of and changes to identification and authentication mechanisms—including but not limited to creation, modification, enabling, disabling, and removal of accounts and modifications of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
		• Initialization, stopping or pausing of the logs. • Creation and deletion of system-level objects. • Setting/modifying logs and logging behavior. • Setting/modifying firewall rules. • Setting/modifying system configurations and parameters. • All password changes. • Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS). • Creation or modification of super-user groups. • Subset of security administrator commands while logged on in the security administrator role. • Subset of system administrator commands while logged on in the user role. • Clearing of the audit log file • Use of identification and authentication mechanisms (e.g., user ID and password) • Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su) • Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system • Changes made to an application or database by a batch file • Application-critical record changes • Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility) • All system and data interactions concerning FTI • System and application alerts and error messages. • System and application shutdown and restart. • Security policy modifications. • Printing sensitive information. • Packet-screening denials originating from untrusted networks. • Packet-screening denials originating from trusted networks. • Modification of proxy services. • Wireless activity.	

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
2	Logging Individual User Access	Log all individual user access to data with a data protection categorization of High.	High
3	Content of Log Records	Logged events must contain the following information: • User identification. • Type of event. • Timestamp using internal system clocks that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). • Success or failure indication. • Identity or name of affected data, file, system component or resource. • Program or command used to initiate the event. • Source and destination addresses.	Low Moderate High
4	Performance Monitoring	Systems must be monitored for system resource utilization and overall system availability to ensure the system meets business availability and performance requirements.	Low Moderate High
5	Security System Failure	Immediately report failures of critical security control systems to security and system support personnel, including failures of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Logging mechanisms • Segmentation controls (if used)	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
6	Security System Failure Response	Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required because of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	Low Moderate High
7	Log Review	Review the following using automated methods, where technically possible, at least daily: • All security events. • Logs of all systems that store, process, or transmit data with a data protection categorization of High. • Logs of all critical system components • Logs of all systems that perform security functions including but not limited to firewalls, intrusion detection systems/intrusion prevention systems, and authentication servers. Review logs of all other system components periodically based on risk. Correlate logs across different repositories to gain enterprise-wide situational awareness. Perform manual reviews of system logs randomly on demand but at least once every thirty (30) days. Exceptions and anomalies identified during the review process must be investigated and security events addressed following the information security incident management process.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
8	Clock Synchronization	Synchronize all system clocks at least hourly to a designated internal time source that is accurate to the approved industry-accepted authoritative time source. Time data must be protected from unauthorized modification. External primary and secondary time servers used must be selected from the National Institute of Standards and Technology (NIST) Internet time service. The secondary server is selected from a different geographic region than the primary server.	Low Moderate High
9	Protection of Logs	Logs must be secured by: • Limiting access to those with a job-related need. • Protecting log files from unauthorized modification or deletion. • Requiring log configuration changes to be approved by authorized security personnel. • Only allowing defined personnel or roles to set or change which events are to be logged by specific systems.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
10	Centralized Log Management Service	An authorized central log server must be in place that: • Collects/receives log data from systems that store, process, or transmit data with a data protection categorization of High. • Collects/receives log data from systems/software that perform security functions including but not limited to firewalls, intrusion detection systems/intrusion prevention systems, authentication servers, and anti-malware software. • Collects/receives log data in as near real time as is appropriate for the log source. • Provides log reduction and normalization. • Does not alter the original content or time ordering of the log data. • Ensures the confidentiality, integrity, and availability of stored logs. • Monitors the availability of log sources. • Alerts authorized security personnel of inappropriate or unusual activities. • Compiles audit records into a system-wide, time-correlated audit trail. • Alerts authorized security personnel when allocated log storage volume is nearing maximum storage capacity.	High
11	Retention of Logs	Retain log data for at least one year, with a minimum of three months immediately available for analysis. Log data for Federal Tax Information (FTI) must be retained for seven years. Sufficient storage capacity must be allocated to ensure log data is maintained for the duration of the retention period. The system must alert incident response personnel within 24 hours of log storage volume reaching 80 percent of the repository's maximum audit record storage capacity.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
12	Change Detection	Centrally managed change detection mechanisms (for example, file integrity monitoring) must be in place to detect and alert on unauthorized changes to: • Critical system files. • Configuration files. • Critical application files. • Security log files. Change detection mechanisms must be configured to perform critical file comparisons at least daily events must be immediately forwarded to an authorized central log server.	High
13	Configuration Checking	Centrally managed configuration checking must be in place to detect and report on system compliance to security configuration baselines.	High
14	Network Intrusion Detection and Prevention	Centrally managed network intrusion detection and/or prevention must be in place to: • Monitor network traffic between different zones of control and between the internet and internal network. Intrusion detection agents must be deployed on the wireless side of the firewall. • Monitor inbound and outbound connections for unusual or unauthorized activity or conditions. • Perform daily system integrity checks of firewalls and other network access control systems. • Network intrusion events must be continuously forwarded to an authorized central log server.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
15	Host Intrusion Detection and Prevention	Host intrusion detection/prevention software must be in place on systems that store, process, or transmit Federal Tax Information (FTI), where technically possible, to monitor for attack attempts and potential compromises. This software must: • Be actively running. • Prevent users from disabling or altering the software. • Generate event logs and continuously forward to an authorized central log management service. • Alert authorized personnel when indications of compromise or potential compromise occur including: • Unauthorized export of information. • Signaling to an external information system. • Potential intrusions. • Be centrally managed.	High
16	Wireless Intrusion Detection	Centrally managed wireless intrusion detection must be in place to identify unauthorized wireless devices and to detect attack attempts and potential compromises to the wireless network. Wireless network intrusion events must be continuously forwarded to an authorized central log server. Where wireless intrusion detection coverage is not in place other processes must be implemented to detect unauthorized wireless access points on a quarterly basis. Incident response procedures must be implemented in the event unauthorized wireless access points are detected.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
17	Anti-Malware Software	Anti-malware software capable of detecting, removing, and protecting against all known types of malicious software and malicious functions within other suspicious files on all systems commonly affected by malicious software and at critical points throughout the network. This software must: • Be actively running. • Prevent users from disabling or altering the software. • Generate event logs and continuously forward to an authorized central log server. • Automatically check for and install updates at least daily. • Perform desktop and critical system file scans as the files are downloaded, opened, or executed. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection. • Be capable of addressing the receipt of false positives. • Be centrally managed.	Low Moderate High
18	Anti-Malware Review	For systems not commonly affected by malicious software, perform evaluations at least annually to identify and evaluate evolving malware threats to confirm whether such systems do not require anti-malware software.	Low Moderate High
19	Inspect Media	Inspect all media containing diagnostic and test programs for malicious code before the media are used in the information system.	Low Moderate High
20	Spam Protection	Centrally managed spam protection mechanisms must be in place at system entry and exit points to detect and act on unsolicited messages. Update spam protection mechanisms when new releases are available following normal change processes.	Low Moderate High

Reason for the Standard

Security monitoring and log management reduces the likelihood that malicious activity would go unnoticed and affect the confidentiality, availability, or integrity of State data and systems.

Roles & Responsibilities

- Employees, Vendors, and Contractors
  - Be aware of and follow relevant information security policies, standards, and procedures.
  - Ensure information security is incorporated into processes and procedures.
  - Ensure vendors and contractors are following required information security controls.
  - Contact information security staff or email GRC@state.mn.us with questions about the information security policies, standards, or procedures.
- Supervisors and Managers
  - Ensure employees and contractors are proficient in the information security policies, standards and procedures that are relevant to their role.
  - Hold employees accountable for following the information security policies, standards, and procedures.
- Information Technology Personnel
  - Apply appropriate controls to the design, operation and maintenance of systems, processes, and procedures in conformance with the information security policies, standards, and procedures.
- Information Security Personnel
  - Develop, maintain, and assess compliance with the information security policies, standards, and procedures.
  - Develop, maintain, and implement a comprehensive information security program.
  - Provide training on information security policies, standards, and procedures.
  - Assist agencies and personnel with understanding and implementing information security policies, standards, and procedures.
- Agency Data Practices Personnel
  - Assist agencies and personnel with questions on proper data use, collection, storage, destruction, and disclosure.

Applicability

This standard applies to all departments, agencies, offices, councils, boards, commissions, and other entities in the executive branch of Minnesota State Government.

Related Information

Security Monitoring and Response Policy

State Standards and Authoritative Source Cross Mapping

History

Table 2. Version History

Version	Description	Date
1.0	Initial Release	7/8/15
1.1	Added Compliance Enforcement Date	12/29/2015
1.2	Updated Compliance Enforcement Date and Template	12/20/2016
1.3	Updated Compliance Enforcement Date and Template	10/26/2016
1.4	New document title and updates for clarification and to include MARS-E requirements	3/10/2020
1.5	Fixed formatting errors and updated required antimalware scanning	11/1/2021
1.6	Scheduled document refresh	10/1/2022
1.7	Updated version number and revision date	10/1/2023
1.8	Added enforcement language; updated version and revision date	12/2/2024
1.9	Removed outdated MARS-E reference	1/12/2026

Contact

GRC@state.mn.us