Network Security 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 Office **Date:** 2/27/2026

Standard Statement

Network security controls must be in place to limit access to only the systems and services necessary.

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. Network Security Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
1	Firewalls	Firewalls must be in place at each Internet connection, between wireless networks and networks containing data with a data protection categorization of High and between any demilitarized zone (DMZ) and internal network zones.	Low Moderate High
2	Firewall Vendors	Firewalls from at least two different vendors must be utilized at the various levels within networks containing systems in scope for ARC-AMPE to reduce the possibility of compromising the entire network.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
3	Network Connection Approval	All network connections and changes to the firewall and router configurations must be tested, justified, communicated, and approved by authorized personnel.	Low Moderate High
4	Firewall and Router Rule Sets	Firewall and router rule sets must: • Restrict connections between lower trusted networks and systems in higher trusted networks. • Restrict inbound and outbound traffic to only that which is necessary and specifically deny all other traffic. Configure these firewalls or routers to permit only traffic necessary for business purposes between the wireless environment and any systems with a data protection categorization of High.	Low Moderate High
5	Rule Set Review	Firewall and router rule sets must be reviewed at least annually. Firewall rules for systems in scope for PCI must be reviewed every six months.	High
6	Unnecessary Rules	Any rules that are no longer needed or justified must be removed.	Low Moderate High
7	Rule Documentation	All services, protocols, and ports used must be documented. Documentation must include: • Business justification. • Duration needed. • Security features implemented for those protocols considered to be insecure. • Business owner contact information. • Technical owner contact information.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
8	Router Configuration Backup	Router configuration files must be secured and backed up.	Low Moderate High
9	DMZ	Inbound Internet traffic must be restricted to a security zone of control that is physically or logically separated from internal networks. The zone must only contain systems that are intended and authorized to be publicly accessible.	Low Moderate High
10	Anti-Spoofing	Anti-spoofing measures to detect and block forged source IP addresses from entering the network must be in place between the internal network and the Internet.	Low Moderate High
11	Outbound Traffic	All outbound Internet traffic must be through a security proxy. Outbound traffic must be limited to only that which is authorized and needed for business purposes.	High
12	Stateful Inspection	Stateful inspection, also known as dynamic packet filtering, must be in place between the internal network and the Internet.	Low Moderate High
13	Network Placement	All systems that store process or transmit State data must be in network zones appropriate for their function and their protection requirements. System components that store data (such as a database) must be in an internal network zone, segregated from the DMZ and other untrusted networks. Key information security tools, mechanisms, and support components associated with system and security administration such as Active Directory Servers, LDAP Servers, DNS Servers, Logging Servers, Patching Servers, etc., must be isolated from other internal information system components via physically or logically separate subnets.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
14	Internal IP Address Disclosure	Network address translation (NAT) or similar methods of masking internal IP addresses must be implemented between the internal network and the Internet.	Low Moderate High
15	Wireless Security	Internal wireless access must be restricted to authorized users with a business need. Only devices that are managed by the State shall be allowed to connect to Internal wireless networks. Internal wireless networks must: • Use the Institute of Electrical and Electronic Engineers 802.11i wireless security standard. • Perform mutual authentication via 802.1X and extensible authentication protocol. • Have service set identifier broadcasting disabled. • Shut down access points when not in use (i.e., nights, weekends). • Utilize MAC address authentication. • Utilize static IP addresses not DHCP.	Low Moderate High
16	VoIP Security	For VoIP systems in scope for IRS regulatory requirements: • VoIP traffic must be physically or logically segmented from other network traffic. • All VoIP communications involving FTI must be encrypted in transit using FIPS 140-2 validated encryption methods. • VoIP traffic must be filtered using VoIP-ready firewalls and inspected for unauthorized access or misuse. Firewalls must be configured to only allow authorized traffic between VoIP devices. • Auditing of VoIP traffic must be enabled to ensure all access to FTI is logged and reviewed regularly for unauthorized activity. • VoIP systems handling FTI must implement access control mechanisms and ensure proper identification and authentication of users.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
17	Publicly Accessible Network Jacks	Network jacks that are in unsecured areas (accessible to the public) must be disabled and only turned on when needed, configured to only allow access directly to the Internet, or configured to only allow approved devices access to the internal network. Any physical ports (e.g., wiring closets and patch panels) not in use must be disabled.	Low Moderate High
18	External File Sharing	Access to file sharing services outside of the State of Minnesota network will be blocked unless such access is approved by management	Low Moderate High

Reason for the Standard

Implementing strong network security controls limits the remotely accessible targets for an attacker. Strong network security also restricts access to sensitive information to only those systems and individuals that have a business need.

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

Enterprise Technical Security Policy

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Table 2. Version History

Version	Description	Date
1.0	Initial Release	7/8/2015
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	10/26/2017
1.4	Changed title of document. Edited for clarity and to include additional MARS-E requirements	3/10/2020

Version	Description	Date
1.5	Scheduled Document Refresh	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; clarified VoIP requirements; updated version and revision date	12/2/2024
1.9	Replaced outdated MARS-E reference with ARC-AMPE	1/12/2026

Contact

GRC@state.mn.us