Network Security

Standard number: DS-14
Date issued: 7/1/2018
Date last reviewed: 2/18/2025
Date last updated: 2/18/2025 (see overview of changes)
Date of next review: 2/18/2027
Version: 2.0
Approval authority: Vice President for Information Technology and CIO
Responsible office: Information Assurance

This Standard supports and supplements the Information Security (SPG 601.27) policy. It will be periodically reviewed and updated as necessary to meet emerging threats, changes in legal and regulatory requirements, and technological advances.

I. Overview

In today's digital world, U-M networks are vital to university operations and life on campus. They support open access to resources across a diverse academic environment, while protecting the university's valuable digital resources and data.
This standard describes the requirements that help to ensure the confidentiality, integrity and availability of network resources. It is essential to:

- Monitor and protect the university's networks, and associated systems, services, and applications, from abuse, attacks, and inappropriate use;
- Take prompt corrective actions to ensure satisfactory mitigation of identified risks to networks;
- Implement safeguards to identify and mitigate threats to the network as a resource, and as a platform of attack against U-M resources, property, or data;
- Effectively balance operational concerns and security challenges.

The underlying principle of this standard is that there is a designated Network Service Provider for each of the three U-M campuses and Michigan Medicine that is responsible for running and approving all network and network security infrastructure components on their campus.

II. Scope

This standard applies to the Ann Arbor campus, Michigan Medicine, UM-Dearborn, UM-Flint, all affiliates, and all faculty, staff, workforce members, and sponsored affiliates. It further applies to:

- All university computer and telecommunications systems, including externally hosted systems;
- Employees, workforce members, contractors, and other delegated agents of the university who manage, administer, and use such systems;
- Any third-party provider with a contractual relationship with the university that has been provided access to the U-M network.

In the context of this standard, network infrastructure resources include but are not limited to:

1. Wired and wireless networks;
2. Communications equipment including, but not limited to, physical networking infrastructure, such as cabling, routers, switches, firewalls and other network protection devices, load balancers, wireless access points, and DHCP and DNS servers, cellular, VoIP and cable TV.

III. Standard

U-M deploys a variety of network monitoring and protection mechanisms that are critical to network security and early threat detection and are designed to:

- Prevent exfiltration or the unauthorized transfer of data;
- Restrict network access to specific hosts and services with failsafes; and
- Limit the attack surface of networked devices.

These mechanisms must be deployed concurrently across the university as multiple, reinforcing layers of network security.

Secure Network Configuration and Management

Installation and maintenance of network infrastructure resources requires prior approval by a Campus Network Service Provider.
University network and system administrators have the individual and collective responsibility to manage U-M networks—wired and wireless—according to the requirements below.

Wired Networks

- Network connectivity devices such as routers, wireless access points, switches and firewalls are securely configured as appropriate to reduce risks to confidentiality, availability, and integrity of U-M systems and data;
- Network is properly documented including security contact information (*VPN connection required when accessing off-campus*) and an up-to-date network map;
- Network-connected devices with services not requiring exposure to the Internet (e.g., printers) should be protected by use of access control lists or by configuring them with private IP addresses;
- Where feasible and appropriate, and to limit the damage that can be done if a vendor is compromised, third party vendors handling U-M data classified as Restricted or High should get remote access to only a specific segment of the network.

Wireless Networks

Wireless networks require special attention to security because data is transmitted using radio signals that can be easily intercepted without proper encryption. To ensure the security of wireless networks, adhere to the following:

- **Consider all wireless technologies, not just Wi-Fi**. There are many wireless technologies including, but not limited to, Wi-Fi, cellular, and bluetooth. Not all are controlled by the university, so beware of using wireless technologies for secure data transfers.
- **Use secure campus Wi-Fi networks, such as MWireless (on campus), whenever possible**. These university-operated Wi-Fi networks meet current industry standards for providing advanced security for wireless users. Ensure that all wireless traffic is encrypted between the user's device and the wireless access points.
- **Do not use the campus MGuest or MSetup Wi-Fi networks for sensitive data**. The campus guest and IoT network do not meet the same security standards as other university-operated Wi-Fi networks and should not be used to transmit sensitive institutional data.
- **Use end-to-end encryption**. Use higher-level protocols such as HTTPS to ensure end-to-end encryption for sensitive data, even after it leaves the wireless network.

Network Access Controls and Firewalls

Network access controls, typically and most efficiently provided by firewalls (both network and host-based), are a critical component to a comprehensive security program and are often called out specifically in compliance regimes. To ensure proper placement, configuration and benefit, firewalls should:

- Be implemented in multiple layers (e.g. host-based and network firewalls) thus exemplifying proper network defense in-depth;
- Be configured with a default deny ruleset, which explicitly denies all traffic unless permitted by previous rulesets;
- Appropriately isolate sensitive data from internal and external non-trusted networks based on risk level;
- Follow the principle of least privilege;
- Log notable activities related to firewall availability and tracking as defined in Security Log Collection, Analysis, and Retention (DS-19);
- Host-based firewalls must be enabled, continuously active, and configured in accordance with industry best practices. Rules for dedicated remote access protocols, such as RDP, SSH, and other insecure remote access protocols should follow the requirements outlined in this standard and Endpoint Security Administration (DS-23).
- Campus Network Service Providers, in consultation with ITS Information Assurance or HITS Information Assurance, reserve the right to block common remote access ports and protocols for security purposes.
- Campus Network Service Providers reserve the right to quarantine or disconnect any system or device from the campus network.

Network Extensions

Extensions include, but are not limited to, remote access Virtual Private Networks (VPNs), site-to-site VPNs, or VPN-like devices and programs, remote access and Remote Monitoring and Management software (e.g. Wireguard, TeamViewer), firewall appliances, routers, switches, hubs, and wireless access points.
To provide the best possible quality of network service, ensure network security and integrity, and minimize the interference between the campus network and other products deployed throughout campus, extensions to the U-M network:

- Must be documented by an Authorized Campus Network Administrator, based on NIST 800-47, Managing the Security of Information Exchanges, then reviewed and approved by a Campus Network Service Provider, in consultation with ITS Information Assurance or HITS Information Assurance, prior to activation.
- Units, research groups, and individuals should not run their own VPN or Firewall without prior authorization from their Campus Network Service Provider.
- Any approved Remote Access VPN servers must utilize two-factor authentication.
- When unapproved network extensions are identified, they will be blocked without notice.

IV. Roles and Responsibilities

The following role-specific responsibilities are intended to help ensure that the confidentiality, integrity and availability of U-M network resources are maintained.

ITS and HITS Information Assurance (IA)

- Establishes network security standards that meet the information security requirements of the university, including those mandated by laws and regulations;
- Establishes appropriate operational controls necessary to mitigate the risks associated with unauthorized disclosure, loss, or theft of university information;
- Collaborates with ITS Network infrastructure and authorized campus network administrators to troubleshoot and resolve network problems and to optimize overall network security;
- Monitors the network to identify and mitigate internal and external intrusions and threats, both as a resource and as a platform of attack, against university resources, property, or data;
- Coordinates the response to IT security incidents, including those involving U-M network breaches, and assists U-M units in their response; IA provides a single institutional point of contact for serious IT security incident communication and response.
- IA, acting on behalf of the university, takes all necessary steps to investigate network security threats and suspected violations of university policies and legal requirements, and to assist appropriate authorities in the investigation of suspected illegal activities.

Campus Network Service Providers

Campus Network Service Providers are designated departments for each university campus and Michigan Medicine:

- Ann Arbor Campus: Information and Technology Services (ITS)
- Dearborn Campus: Information and Technology Services (ITS) and UM-Dearborn Information Technology Services
- Flint Campus: UM-Flint Information Technology Services
- Michigan Medicine: Health Information Technology & Services (HITS)

The campus Network Service Provider:

- Serves as authoritative network administrator for their campus.
- Provides network security capabilities and services in consultation with IA, such as firewalls, VPNs, network border security, WiFi standards, cellular standards, and security, and administrative controls to protect the network.
- Coordinates network performance, disruption or degradation protection capabilities, or any other interference with normal functioning of the network.
- Reviews and approves all network and security infrastructure components to the network.

Authorized Campus Network Administrators

Operational network security responsibilities are authorized based on campus location. Campus Network Service Providers for the Ann Arbor, Dearborn, and Flint campuses and Michigan Medicine are primarily responsible for the day-to-day operation of the campus network and backbones.

Authorized Campus Network Administrators are unit IT staff members designated by ITS Network Infrastructure or IT leaders in their units to support networks within their departments. ITS Network Infrastructure maintains a list of Authorized Campus Network Administrators for communication and

network access purposes. Unit IT leaders are responsible for informing ITS Network Infrastructure of changes to their Authorized Campus Network Administrators.

Authorized Campus Network Administrators:

- Support network and system administrators across the institution; coordinate, manage, and maintain the networking infrastructure, campus backbones, and related services for the university; and administer firewalls and intrusion prevention and detection systems;
- Are responsible for ensuring that all network security standards (both policy and technical) are applied to hosted services;
- Provide ongoing security monitoring for all installed wired and wireless network devices;
- Serve as the authoritative and responsible staff for the registration and management of all university-owned DNS domains;
- Serve as the authoritative and responsible staff for the registration and management of all university-owned public IPv4 and IPv6 address space, as well as all private IP address space used on U-M campuses.
- Document and support the review of interconnects and extensions to the network; upon approval from ITS Network Infrastructure of network interconnects and extensions, ensure their ongoing monitoring and maintenance.

End Users

All U-M faculty, staff, and students using U-M network resources are responsible for all activities on U-M networks that originate from their U-M computing account and devices registered on the network. End users must:

- Adhere to all established network security standards and university policies, including Responsible Use of Information Resources (SPG 601.07);
- Obtain approval by ITS Network Infrastructure for any extension of the U-M network, both wired and wireless;
- Not provide network access to unauthorized individuals;
- Not attempt to cause harm or do anything that can be reasonably perceived as malicious while on a campus network.
  In addition, students who live in university housing must adhere to the U-M Network Responsible Use Agreement.

V. Violations and Sanctions

Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the U-M network. The university may require specific security improvements to address identified problems before the device may be connected.

Violations of this Standard may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non-reappointment, discharge, dismissal, and/or legal action. In addition, the connectivity of machines and servers to the U-M network that do not comply with this Standard may be limited or disconnected.

Discipline (SPG 201.12) provides for staff member disciplinary procedures and sanctions. Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable university procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in Regents Bylaw 5.09. In addition to U-M disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

Any U-M department or unit found to have violated this policy may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

VI. Implementation

Information Assurance is responsible for the implementation, maintenance, and interpretation of this Standard.

VII. References

- Responsible Use of Information Resources (SPG 601.07)
- Information Security Policy (SPG 601.27)
- Security Log Collection, Analysis, and Retention (DS-19)
- Endpoint Security Administration (DS-23)
- U-M Network Responsible Use Agreement
- ITS Wi-Fi and Networks, Network Security
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems

VIII. Related NIST Security Controls

- NIST SP 800-53 Revision 5
  - AC-06 Least Privilege
  - AC-18 Wireless Access
  - SC-07 Boundary Protection
  - SC-08 Transmission Confidentiality and Integrity