SUBJECT:	Information Technology				
POLICY:	701.1 Campus Networking				
PROCEDURE:					
EFFECTIVE:	November 2003	**REVISED:**	July 2014	**REVIEWED:**	November 2022

Introduction and Purpose

Great Falls College MSU relies on secure, reliable, and centrally managed network services to support instruction, student services, administration, communication, public safety, research, and business operations. The campus network includes voice, video, data, wired, wireless, remote access, cloud-connected, and network infrastructure services used to conduct college business.

The purpose of this policy is to establish requirements for governance, management, protection, monitoring, and appropriate use of the Great Falls College MSU network. This policy supports the confidentiality, integrity, availability, and resiliency of institutional systems and data by requiring appropriate network oversight, access control, device management, security monitoring, change management, and risk-based exceptions.

This policy is aligned with recognized cybersecurity risk management practices, including the National Institute of Standards and Technology Cybersecurity Framework and applicable NIST security and privacy control guidance.

~~To ensure the integrity, privacy, and security of Great Falls College MSU' campus electronic information, the campus voice, video, and data network is managed centrally by the Information Technology Services Department (ITS).~~

Policy

The Great Falls College MSU campus network ~~includes~~shall ~~both~~be ~~wired~~centrally ~~and~~managed ~~wireless~~by ~~components.~~Information Technology Services. Any ~~wired~~wired, wireless, virtual, cloud-connected, or ~~wireless~~remote ~~devices~~access device, service, or ~~networks~~system that ~~are~~connects ~~connected~~to, ~~to~~transmits over, extends, manages, or affects the campus network ~~backbone are considered part of the campus network and are~~is subject to this policy, regardless of ~~their~~ ownership.

Information Technology Services has authority to approve, deny, restrict, disconnect, quarantine, monitor, or remove network-connected devices, services, or systems when necessary to protect college systems, data, users, operations, or network availability.

Scope

This policy applies to:

All Great Falls College MSU network infrastructure including wired, wireless, voice, video, data, remote access, and cloud-connected network services.

All college-owned, personally owned, vendor-owned, contractor-owned, temporary, or guest devices that connect to the campus network.

All endpoint devices, including but not limited to workstations, laptops, tablets, mobile devices, printers, phones, cameras, servers, lab systems, instructional technology, Internet of Things devices, and operational technology.
All network devices, including but not limited to switches, routers, firewalls, wireless access points, wireless controllers, gateways, repeaters, DHCP services, DNS services, NAT services, VPN services, and related hardware, software, or virtualized systems.
All users of the campus network, including employees, students, guests, vendors, contractors, affiliates, volunteers, and other authorized users.

Network Governance and Authority

Information Technology Services serve as the central authority for the campus network. Network design, addressing, segmentation, authentication, routing, switching, wireless services, firewall rules, remote access, monitoring, and related network services must be managed or approved by Information Technology Services.
No department, employee, student, vendor, contractor, or guest may install, connect, configure, or operate network infrastructure or network services without prior approval from Information Technology Services. This requirement applies to all device and service categories identified in the Scope section above, including but not limited to:
Switches
Routers
Wireless access points
Firewalls
DHCP/DNS/NAT services
VPN services
Cellular routers or hotspots used to bypass college network controls
Information Technology Services may immediately restrict, disable, quarantine, or disconnect any device, service, connection, or user account that presents unacceptable risk to the confidentiality, integrity, availability, security, or stability of college systems, data, users, or operations.

Network Device Requirements

Network devices may only be installed, connected, configured, operated, or managed by Information Technology Services or by another party with documented approval from Information Technology Services.
Network devices must meet college technical, operational, and security standards before being connected to the campus network. These requirements may include, but are not limited to:
Secure configuration
Supported hardware, firmware, and software
Current security updates
Approved management access
Logging and monitoring capability

Strong authentication
Encrypted administrative access where supported
Documented ownership and support contacts
Compatibility with college routing, switching, wireless, addressing, and security architecture
Restrictions on unmanaged or unsupported services
Compliance with applicable legal, regulatory, contractual, and policy requirements
Network devices that are unsupported, misconfigured, compromised, vulnerable, undocumented, or unauthorized may be restricted, disconnected, isolated, or removed.

Network Segmentation and Access Control

Information Technology Services may segment the campus network based on institutional role, user type, device type, location, ownership, business function, data sensitivity, compliance requirement, or risk level.
Access between network segments must be limited to approved business or educational purposes. Access controls may include firewalls, access control lists, network access control, authentication requirements, device classification, VLANs, routing restrictions, security groups, or other technical controls.
Administrative, server, security, building systems, public safety, regulated data, IoT, guest, lab, classroom, and public networks may be separated to reduce risk and support operational stability.
Information Technology Services may require devices or systems to use restricted network segments, limited access rules, compensating controls, or enhanced monitoring based on risk.

Guest and Public Network Access

Guest and public network access may be provided for visitors, events, or other approved purposes. Guest access does not imply access to internal college systems or protected institutional resources.
Guest network services may be limited by bandwidth, duration, authentication method, content filtering, segmentation, monitoring, or other operational and security controls.
Guest users must comply with applicable college policies and may have network access restricted or revoked at any time.

Monitoring, Logging, and Privacy

Network-connected devices, services, authentication events, traffic patterns, security alerts, and system logs may be monitored, collected, retained, reviewed, or analyzed as permitted by applicable law, college policy, Montana Board of Regents policy, and operational need.
Monitoring may be conducted to:
Maintain network availability and performance
Troubleshoot technical issues
Detect unauthorized devices or services
Investigate security events
Protect institutional systems and data
Support compliance obligations
Prevent or respond to misuse

Support incident response and recovery
Users should have no expectation that use of the campus network is private when using college systems or network services, except as provided by applicable law, policy, or regulation.

Exceptions and Risk Acceptance

~~Any device to be directly connected (wired) to the network must be approved by IT before it is connected. All network- connected devices (wired or wireless) are subject to monitoring per Montana Board of Regents policy.~~

Exceptions to this policy ~~may~~or related standards must be ~~granted,~~documented ~~when~~and ~~judged appropriate,~~approved by ~~the Director of~~ Information Technology ~~or~~Services ~~the CEO/Dean~~leadership or ~~designee.~~another designated authority.

Exception requests must include:
Description of the requested exception
Business or instructional justification
Affected system, device, service, or user group
Data involved, if applicable
Known risks
Proposed compensating controls
Responsible owner
Review date or expiration date
Remediation plan where appropriate
Approved exceptions may require segmentation, monitoring, limited access, compensating controls, time limits, or periodic review.
Exception requests involving regulated data (including but not limited to FERPA-protected records, HIPAA-covered data, payment card data subject to PCI-DSS, or other legally protected categories of data) must be escalated to Information Technology Services leadership and, where appropriate, institutional compliance or legal counsel, prior to approval.
Exceptions may be denied, revoked, or modified if risk changes or if the exception creates unacceptable operational, security, compliance, or privacy concerns.

Enforcement

Violations of this policy may result in restriction, quarantine, disconnection, removal, or denial of network access.
Information Technology Services may take immediate action when a device, service, connection, or user presents risk to network availability, institutional data, college systems, users, or operations.
Policy violations may also be referred for appropriate administrative, disciplinary, contractual, or legal action in accordance with applicable college policies, student conduct processes, employee procedures, contracts, or law.

Definitions

For purposes of this policy, the following definitions apply.

Campus network: the college-managed wired, wireless, voice, video, data, remote access, cloud-connected, or virtual network environment operated for Great Falls College MSU business or educational purposes.

Network device: any physical, virtual, software-based, or cloud-connected device or service that connects, routes, switches, filters, bridges, extends, translates, assigns, broadcasts, authenticates, encrypts, monitors, or manages network traffic.

Unauthorized network device: any network device or network service installed, connected, configured, or operated without prior approval from Information Technology Services.

Institutional data: data created, received, maintained, processed, or transmitted by or on behalf of Great Falls College MSU.

Regulated data: institutional data subject to specific legal, regulatory, or contractual protection requirements, including but not limited to education records under FERPA, protected health information under HIPAA, payment card data under PCI-DSS, and other data categories designated as regulated by applicable law or college policy.

Compensating controls: alternative security measures implemented to reduce risk when a primary control cannot be applied, such as enhanced monitoring, restricted network segmentation, additional authentication requirements, or limited access windows.

Operational technology: hardware and software used to monitor, control, or automate physical devices, processes, or infrastructure, including but not limited to building automation, access control, surveillance, and industrial control systems.

Guest network: a network service intended for temporary or limited access by visitors, guests, or other non-institutional users, subject to restrictions established by Information Technology Services.

Designated authority: an individual formally authorized in writing by Information Technology Services Leadership to approve, deny, or modify exceptions or enforcement actions under this policy.

Roles and Responsibilities

Information Technology Services

Information Technology Services is responsible for:

Designing, operating, maintaining, securing, and monitoring the campus network.

Establishing network architecture, security controls, connection requirements, and configuration standards.

Approving or denying network connections, network devices, wireless services, remote access methods, and third-party connectivity.

Maintaining appropriate documentation for network infrastructure, approved services, and significant network changes.

Monitoring network activity as permitted by applicable law, policy, and Montana Board of Regents requirements.

Responding to network security events, outages, vulnerabilities, unauthorized devices, and policy violations.
Establishing procedures, standards, and technical requirements to support this policy.

Departments

Departments are responsible for:
Consulting with Information Technology Services before purchasing, installing, or connecting devices or systems that require network access.
Ensuring that department-owned or department-managed technology complies with college network requirements.
Identifying systems that may process, store, or transmit sensitive, regulated, confidential, or mission-critical data.
Supporting remediation when devices or systems present security, operational, or compliance risks.
Ensuring that vendor or contractor network access is requested and approved before use.

Users

Users are responsible for:
Using the network in accordance with college policy, applicable law, and acceptable use requirements.
Not installing, connecting, or operating unauthorized network devices or services.
Reporting suspected unauthorized network devices, abnormal network behavior, or security concerns to Information Technology Services.
Following instructions from Information Technology Services related to network security, device configuration, remediation, or access restrictions.

Vendors and Contractors

Vendors and contractors are responsible for:
Obtaining approval before connecting any device, service, system, or remote access method to the campus network.
Using only approved access methods and limiting access to the approved business purpose.
Complying with college security, privacy, monitoring, and network requirements.
Cooperating with Information Technology Services during troubleshooting, security review, incident response, and access termination.

Related Manuals or Forms

~~Related~~
Montana Board of Regents policy 1302 – Privacy, Security, and Monitoring