ENTERPRISE IT STANDARDS AND PROCEDURES
MSU Networking Standards

Policy:	**Technology Management Policy**
Document:	**Technology Management Standards**
Campus:	**MSU-Bozeman**
Revision:	**1.0**
Contact:	**Jerry Sheehan | Chief Information Officer** **jsheehan@montana.edu**

These Standards establish minimum guidelines for management of devices connecting to MSU's network as outlined in the University Technology Management Policy (http://www.montana.edu/policy/enterprise_it/technology_management.html).

Networking Devices:

Devices connecting to the University network must meet the following minimum requirements or have an approved exception from ITC.

MSU current network standards are below. Please be sure to check back regularly as changes in technology will necessarily update these standards:

Networking Devices: Networking devices are any electronic device that connect any other device to the MSU network. These may exist in software (virtualized), hardware or both. Only MSU networking staff are permitted to connect network devices to the MSU network. Examples of these types of devices include, but are not limited to:
- Hubs
- Switches
- Routers
- Wireless Access Points
- Wireless Controllers
- DHCP Servers or services.
- Firewalls
- Gateways
- Repeaters
- NAT (Network Address Translation) devices or services
- Multiplexers

Standards for Endpoint Devices:

Endpoint devices connecting to the MSU network must meet the following standards for compatibility and support. Devices not meeting these standards will not be permitted on the MSU network without an approved exception from ITC.

Endpoint Devices are network connected devices that use the network only for themselves (not a networking device) and must follow the standards below. Please check back regularly as changes in technology will necessarily update these standards:
- Endpoint devices just auto-negotiate connection speed
- Endpoint devices must conform to IEEE 802.3 Ethernet standards
- Endpoint Devices must be able to use and be configured for Dynamic Host Configuration Protocol (DHCP).
- Endpoint Devices must be IPv4 compliant
- Endpoint Devices must be IPv6 compliant or have a roadmap to be so with a published date.
- Endpoint devices must use TCP/IP as a network transport. Exceptions must be approved by ITC.
- Endpoint Devices must be able to be configured via NTP or PTP for time.
- Endpoint Devices must be connected and configurable over Layer 3 of the OSI model. Layer 2 only devices are not permitted.
- Endpoint Devices that use Power over Ethernet (PoE) must conform to Cisco PoE as well as IEEE 802.3af or 802.3at requirements.

Endpoint Devices Configuration Requirements

When endpoint devices are connected to the MSU network the following guidelines will be followed. For any questions, please contact the ITC service desk to get clarification.
- IP addresses are assigned via ITC – you must use only the addresses assigned to you or your device. This may involve changing a device IP address in order to keep it communicating with MSU network configurations.
- IT may put Quality of Service (QoS) features on your connection to ensure network stability.
- IT may put bandwidth quotas on your connection to ensure network stability.
- IT may require some form of connection security (802.1x) for your device to ensure network stability.

Wireless Communications

Devices using wireless communications are included under network devices and will be installed or managed by UIT unless agreed to by UIT network manager or higher. This includes any devices operating at or near the wireless communication spectrum in use by the University even if those devices do not connect to the MSU network.