

Network Connection Policy

This policy describes the requirements and constraints for attaching a computer to the Montana Tech local area network (LAN). All computers installed on the Montana Tech network fall under the authority and responsibility of Network Services and as such they must meet minimum-security requirements. The security requirements, practices, and policies at Montana Tech are available on-line at <http://www.mtech.edu/NetServe/layout.htm>.

The intent of this policy is to ensure that all systems installed on the Montana Tech network are maintained at appropriate levels of security while at the same time not impeding the ability of Montana Tech users and support staff to perform their work.

Question or concerns regarding Montana Tech security can be sent to the Montana Tech CSO.

1.0 System Types

1.1 Secured system

A secured system is fully supported by the Montana Tech support staff, who ensures it meets all of the Montana Tech security requirements.

1.2 Unsecured Systems

An unsecured system is not directly supported by the Montana Tech support staff. An unsecured system may be installed on a separated subnet (DHCP) and is part of a specific subdomain of the domain. The primary user of the system, or someone they designate, is responsible for the integrity of the system and will ensure the system meets the connection-of-service terms. Unsecured systems are treated as untrusted hosts by the secured systems and are viewed, as much as possible, like any other system on the Internet. Unsecured systems are not provided all of the services that are provided to secured systems

The primary user is responsible for ensuring that the agreed security measures and connection terms are put in place, operational, and adhered to. Any security incident occurring on a secured or unsecured system on the Montana Tech network can adversely affect the security of other Montana Tech systems or impact the reputation of the Montana Tech facility, and as such,

will be resolved under the direction of the Montana Tech CSO.

2.0 Minimum Network Hook-up Requirements for Secured Systems

The requirements listed below are the minimum requirements which must be satisfied before a new host can be connected on the network as a Montana Tech-secured system.

2.1 Designation of Support Group or Responsible Person

Each computer attached to the Montana Tech network has an assigned group Coordinator or support person who provides full support for the system and is responsible for ensuring the requirements of this policy are met. In addition, the responsible person or group ensures that the security of the system is maintained by installing needed security patches and security checking programs, and virus scanner updates. The person or group who is responsible for support must have full access to the system. Since a security incident on a Montana Tech-secured system may have an impact on other Montana Tech-secured systems, the responsible person or group must be reachable 24 hrs/day, 7 days/week in the event of a major security incident.

2.2 Notification of New System Installation

Montana Tech Network Services must be notified each time a new host is added to the network. Prior to connection on the network, a valid IP address number must be assigned by network. An IP address number can be obtained by sending email or leaving voice mail for the CSA. As part of the IP address request, the requestor must specify the new host as Montana Tech-secured. The support status of the systems must be included when the notification is given to Network Services. All other Montana Tech support personnel will be notified as appropriate.

2.3 Required Account(s)

Each Montana Tech-secured computer attached to the Montana Tech network must have a Network Access Operations and/or Maintenance account to allow members of the support team access to the system in the event of a problem or to perform routine system functions.

2.4 Root Access

Passwords to special privileged accounts for all computers attached to the Montana Tech network must be documented in a

secure location. The root and other special access passwords for secured systems should be assigned based upon Montana Tech security policies. Periodic system access checks must be made to ensure conformance. All accounts on the system must have a password.

2.5 Standard Montana Tech Domain User ID's

All accounts installed on systems on the Montana Tech Network must be assigned a valid user ID which is unique to that account and user. Valid Montana Tech user IDs can be obtained from Network Services.

2.6 Standard Montana Tech Network Parameters

All hosts in the Montana Tech must obtain a valid network number from Network Services. No host on the network should emit dynamic routing information (RIP, OSPF, etc.) except specially configured by Network Services. Proxy ARP is currently not supported.

3.0 Minimum Network Hook-up Requirements for Unsecured Systems

The requirements listed below are the minimum requirements which must be satisfied before a new unsecured host can be connected on the Montana Tech network. For example devices connected at Residence Hall, Married Students Housing, and other locations such as conference rooms and offices where "personal" computers are connected long term or short term to the network.

3.1 Designation of Support Group or Responsible Person

Each unsecured computer connected on the network must have an assigned group or individual who provides full administrative support for the system and is responsible for ensuring the requirements of this policy are met. If the responsible person is not reachable in the event of a major security problem, then the system will be powered down until approval to return to service is given by the CSO.

3.2 Notification of New System Installation

The appropriate personnel must be notified each time a new host is added to the Montana Tech Network. Unsecured systems are normally configured dynamically with DHCP. Computers naming

conventions must be adhered to. Failure to comply may involve suspension of access until the naming status is remedied.

3.3 Root Access

Where appropriate the password for special/privileged accounts on unsecured systems will be provided to the Montana Tech CSA. All accounts on the system must have a password.

3.4 Standard Montana Tech Network Parameters

All hosts in the Montana Tech domain must obtain a valid network address from Network Services. Dynamic host configuration (DHCP) will supply necessary parameters. No host on the network should emit dynamic routing information (RIP, OSPF, etc.) except those specially configured by Network Services. Proxy ARP is currently not supported.

3.5 Verification of Unsecured Systems

All unsecured systems must undergo a minimum security verification process prior to connection to the Montana Tech Network by appropriate support personnel. In addition, the Montana Tech CSA, or someone designated by the CSA, will be responsible for verifying that conditions outlined in this policy have been met, as well as any additional conditions specified by the Montana Tech CSO. Initial verification by the Montana Tech CSA will be made in a reasonable time frame. Re-verification can be done at any time by the Montana Tech CSA or someone the designate. Re-verification will be done periodically.

.

3.6 Recommended Requirements

In addition to the above listed requirements, it is recommended that users/owners of unsecured systems follow the Montana Tech standard for assignment of user Ids and computer naming conventions. User/owners must run the available security utilities used on Montana Tech-secured system such as virus scanners.

Approved by:

Concurrence: