Information Technology Services

Network Policies

University of Missouri-St. Louis Information Technology Network Usage Policy

The University of Missouri-St. Louis (UMSL) campus network provides access to the campus computing facilities. All users of the UMSL network must conform to the University of Missouri-St. Louis Acceptable Use Policy (http://www.umsl.edu/technology/policy/acceptable.html). Upon connecting a computer to the UMSL network, there are additional policies that must be followed. Violation of any of the following policies may result in immediate disconnection from the network.

Network Usage:

- All UMSL network traffic to and from the Internet must go through the firewall. Any network traffic going around the firewall must be accounted for and explicitly allowed by the Computer Security Incident Response Team (CSIRT).
- Computer security incidents and abuses can be reported to the CSIRT at csirt@umsl.edu , or call the Technology Support Center (TSC) at 314-516-6034.
- Applications which transmit sensitive information over the network in cleartext, such as telnet and ftp, are prohibited and will be blocked. Exceptions must be accounted for and explicitly allowed by the CSIRT. Secure free replacements to telnet and ftp are SSH and SFTP.
- UMSL has enabled port locking which locks a specific PC to a specific network port. Moving a PC to another port, or plugging a new PC into an old PC's port will result in an automatic disabling of that port. This will require a port reset; please call the TSC if that is the case.
- All devices allowed on the campus network (UMSL owned, student owned and allowed guests) must register to Bradford.
- Users may not go outside UMSL for network connectivity, such as signing up for a connection to an outside Internet Service Provider, without the consent of Information Technology Services (ITS).
- Activities that inhibit the ability of others to connect to or use the network are prohibited. This includes, but is not limited to: unauthorized file-sharing, initiating denial of service attacks, initiating viruses or worms, and network scanning.
- ITS will attempt to satisfy all requests for special network topologies that are needed for research or teaching. There may be costs associated with these accommodations.
- For faculty and staff, a fee is associated with any active network port unless it is being used for a printer.

Workstation Configuration and Network Administration:

- Faculty and staff computers running Windows must be joined to the Domain. Exceptions must be approved by ITS.
- Faculty and staff computers must run current campus anti-virus software.
- Servers managed by faculty or staff must be network secured by the responsible party.
- Students may not provide accounts, disk storage, or web pages for other users.
- Users may not set up servers without written approval of the ITS Security Team. This includes but is not limited to DHCP, DNS, WINS, FTP, Web, or Mail servers.
- By default, IP addresses are automatically assigned by Dynamic Host Configuration Protocol (DHCP). The use of a hard-coded or non-approved IP address is prohibited. IP addresses can change without notice unless arrangements are made with ITS to assign a static IP.
- A computer should not be connected to the network via wired connection and wireless connection at the same time.

- Network administration tools are not allowed without written approval of the ITS Security Team. This includes, but is not limited to:
  - Network monitors
  - Sniffers
  - Vulnerability scanners
  - Port scanners
  - SNMP tools

Network Hardware:

- University computing equipment must not be tampered with in any way.
- Wiring may not be split, re-wired, or re-configured.
- Mini-hubs, routers, switches, bridges, wireless access points, wireless bridges, or other network hardware are not allowed.
- Only one computer at a time may connect to each in-room jack.
- A PC with multiple network cards is not allowed to function as a network address translation gateway. For example, Windows Internet Connection Sharing is prohibited. No device other than an ITS device will be permitted to route or bridge packets.
- A PC with a wireless card may not be configured to act as a wireless access point.

Network Maintenance Window:
Sunday mornings from 6:00am-12:00pm are reserved for network maintenance. Every effort will be made to give prior notice. The network and or servers may be unavailable during this time so updates can be made. Access to the network may be suspended to preserve the integrity of the network.

Temporary Guest Accounts:
Non-UMSL users may be granted a temporary guest account with approval by ITS to help facilitate collaboration with researchers at other Universities and sites. These accounts will be allowed to VPN into UMSL. A faculty member must request the account, fill out a form which can be located at https://tomsawyer.umsl.edu/webapps/sso/apps/Generic/login.cfm , and be responsible for the account's usage.

Individual Responsibility for Security on the Student Network:
Users in UMSL student housing are expected to take reasonable steps to ensure that their computer systems do not create a security risk when connected to the network. This includes but is not be limited to the following steps:

- Users must register their computer on the student network using an SSO/ MyGateway username and password.
- Computers must run anti-virus software with current virus definitions.
- Operating systems and software must be kept current with the latest patches and service packs offered by the vendors.
- All accounts on student owned machines should have passwords.
- It is recommended that individual computers be protected by a personal firewall.
- It is recommended that users perform regular scans for malware using anti- spyware software.