



Responsible Use of University Computing Resources Policy Document

Network Access and Usage

1.0 Purpose

This policy is designed to protect the campus wired and wireless networks and the ability of members of the Montclair State community to utilize network services. The purpose of this policy is to define the standards for connecting computers, servers or other devices to the University's wired and wireless network. The standards are designed to minimize the potential exposure to Montclair State University and our community from damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance.

Montclair State University must provide a secure network for our educational, research, instructional and administrative activities. An unsecured and/or unregistered device on the campus network could allow denial of service attacks, viruses, Trojans, and other malicious activity to compromise the University's campus network, thereby affecting many computers, devices, and services. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical Montclair State University internal systems. Universities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the Montclair State network must follow specific standards and take specific actions.

2.0 Scope

This policy applies to all members of the Montclair State University community or visitors who have any device connected to the Montclair State University network, including, but not limited to, desktop computers, laptops, servers, wireless computers, tablets, streaming media players, gaming systems, specialized equipment, cameras, printers, environmental control systems, and telephone system components. This policy also applies to anyone who has systems outside the campus network that access the campus network and resources. The policy applies to any University-owned devices (including those purchased with grant funds), and personally-owned or leased devices that connect to the Montclair State network.

3.0 Policy

3.1 Appropriate Connection Methods

You may connect approved devices to the campus network at appropriate connectivity points including voice/data jacks, through a University-operated wireless network access point, via a VPN or SSH tunnel, or through remote access mechanisms such as residential ISPs, DSL, cellular data networks, and traditional modems over phone lines.

Modifications or extensions to the campus network can potentially cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of the modification. Therefore, extending, disabling, or modifying the Montclair State network in any way is strictly forbidden. Exceptions may be granted by IT for approved personnel in departments who can demonstrate competence with managing the aforementioned hardware and software, and who agree to abide by all IT networking standards and practices.

3.2 Network Registration

Any user who wishes to connect a device to the campus network must first register that device using the IT NetAccess systems. The NetAccess system requires that a user enter their valid MSU NetID and password and then performs an automated scan of the device for known security vulnerabilities. If the security scan is successful, the device is registered with the campus DHCP service.

The NetAccess system maintains a database of unique machine identification (MAC address), network address (dynamic IP) and owner for the purposes of contacting the owner of a computer when it is necessary. For example, IT would contact the registered owner of a computer when his or her computer has been compromised and is launching a denial of service attack or if a copyright violation notice has been issued for the IP address used by that person's device..

Devices which cannot utilize the NetAccess system for network registration (i.e. printers) must be registered manually by IT. Users of such devices should place a call or email the Help Desk (x7971, helpdesk@mail.montclair.edu) and include the devices make, model, hardware MAC address, location, and owner information.

Users may not, under any circumstances, arbitrarily assign a University IP address (130.68.x.x) or domain name (*.montclair.edu) to a device without prior authorization from IT.

3.3 Responsibility for Security

Every computer or other device connected to the campus network must have an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer in her office, or IT in the case of devices in public computer labs.) In the context of this policy document, owners and caretakers are both referred to as owners.

Owners are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to their Departmental or College Technology Support group. Therefore, it is possible that one owner manages multiple departmental machines plus his or her own personal computer. Every owner should know who is responsible for maintaining his or her machine(s).

3.4 Security Standards

These security standards apply to all devices that connect to the Montclair State University network through standard university ports, through wireless services, and through home and off campus connections.

- Owners of departmental servers that are connected to the campus network must provide central IT with the 'administrator' or 'root' password to the device, or an account with equivalent privileges. This account will be used only by full-time IT security personnel to ensure the security and integrity of the device via routine, coordinated system scans or other non-intrusive mechanisms. Under no circumstances will IT use the administrator/root account to manage the departmental device or perform any activity that would potentially compromise its intended functionality or expected performance.
- Owners must ensure that all computers and other devices capable of running anti-virus software have Montclair State-licensed anti-virus software (or other appropriate virus protection products) installed and running. The anti-virus software must be configured to automatically update its virus definition files at least once per hour if it does not incur significant network or CPU overhead. See IT's software site for more information on campus licensed anti-virus products.
- Computer owners must install the most recent security patches on their system as soon as practical or as directed by IT. It is recommended that automatic software updates be configured on operating systems that support such a feature. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.
- In general, sensitive University data may NOT be stored on computing devices other than IT-owned and operated servers and storage devices. If sensitive data must be stored on a non-IT server or storage device, then that data must be encrypted to prevent unauthorized access in the event the device is compromised or stolen. Please refer to the [Data Classification and Handling](#) policy document for additional details.

3.5 Centrally-Provided Network-Based Services

IT, the central computing organization, is responsible for providing reliable network services for the entire campus. As such, individuals or departments may not run any service which disrupts or interferes with centrally-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions may be made by IT for approved personnel in departments who can demonstrate competence with managing the aforementioned services.

Individuals or departments may not attach routers, switches, hubs, or wireless access points to the campus network without prior approval from IT.

Individuals or departments may not run any service or server which requests from an individual their IT-maintained credentials (ex NetID and password) unless the username/password entry and lookup is occurring over a secure channel to an IT-maintained directory service. Please refer to the [Secure Directory Services Access](#) policy document for additional details.

3.6 Protection of the Network

IT routinely scans the Montclair State network, looking for vulnerabilities and rouge (unregistered)

devices. By connecting a computer or device to the campus network, you are acknowledging that the network traffic to and from your computer may be scanned at the packet level according to criteria such as source/destination addressing, protocol, bandwidth consumption, etc.

IT reserves the right to take necessary steps to contain security exposures to the University and mitigate the impact of improper or disruptive network activity. In order to allow normal traffic and central services to resume, IT will take action to contain devices that exhibit the behaviors indicated below:

- imposing an exceptional load on a campus service.
- exhibiting a pattern of network traffic that disrupts centrally provided services.
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others.
- exhibiting behavior consistent with host compromise.

IT reserves the right to restrict certain types of traffic coming into and across the Montclair State network. IT restricts traffic that is known to cause damage to the network or hosts on it. IT also may control other types of traffic that consume too much network capacity, such as file-sharing traffic. Please refer to the Montclair State University's [Responsible Use of University Computing Resources](#) policy document for further details.

4.0 Related Policies & Links

1. Account Management Policy
2. Data Classification and Handling Policy
3. Security Directory Services Access Policy
4. Responsible Use of University Computing Resources Policy

Revision History

rev 1.0 11/13/13 Initial release