Network Access Policy

Purpose

The purpose of the Muskegon Community College Network Access Policy is to establish the rules for the access and use of the Muskegon Community College network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of Muskegon Community College's information.

Audience

The Muskegon Community College Network Access Policy applies equally to all individuals with access to any Muskegon Community College Information Resource.

Policy

- Computers and peripherals that connect the college's internal network must be college owned, managed by OIT, and conform to all applicable Muskegon Community College IT standards. Computers that do not meet standards must utilize an alternate network, i.e. guest network, or open wireless network. These standards include but are not limited to the following:
    - Computers and peripherals are inventoried according to asset guidelines (i.e. asset tags, location, etc.)Computers and peripherals are moved by OIT according to equipment move guidelines to maintain accurate inventory.
    - Computers are patched and updated by OIT, through central software updating services when possible. Computers are provided with updated virus protection software, through central virus protection management when possible.
    - For systems with Microsoft Windows operating system, computers are supplied with group policies through the MUSKEGONCC domain (with the exception of lab computers for networking classes).
    - Computers and peripherals are permitted to access the college's networks using only the network and host addresses issued to them by Muskegon Community College IT.
    - Access to resources through the Muskegon Community College's internal network requires unique, named network accounts. Ownership

of each account must be documented and anonymous access is not permitted.

- o Users must not download, install or run security programs or utilities designed to scan for security vulnerabilities, or exploit resources.
- o A secure connection to another private network is prohibited while connected to the Muskegon Community College corporate network unless approved in advance by Muskegon Community College IT management.

- **Penalties for Misuse**

Misuse can lead to penalties up to and including loss of system access, employment termination, expulsion from classes or from the college, and may also lead to a requirement to repay costs associated with any damages caused to the College or other users. In addition, some activities may lead to risk of personal legal liability, both civil and criminal, under local, state and federal laws and regulations.

Definitions

1. **Internal Network:** A collection of computers and peripherals, connected to each other and all internal college resources. Access to services is based on user permissions rather than separating networks. In addition to Internet connectivity, internal services such as printing, home directory, shared department directories, internal email, and administrative systems are available.
2. **Guest Network:** A collection of computers and peripherals connected to the internal network through a protected connection. Access to internal resources is limited and secured to protect internal resources. Users can expect to have access to the Internet, Internet email, and Internet based access to your home directory, but not access to printing or shared directories.
3. **Open Wireless Network:** An open, community access network designed for Internet connectivity.