INFORMATION SECURITY
Network Access and Management

2.25062 DP
DISTRICT PROCEDURE

PURPOSE

The purpose of this procedure is to ensure the effective management and security of Metropolitan Community College's (MCC) networks.

APPLICABILITY

This procedure applies to all students, employees, and visitors to MCC.

DEVICE ATTACHMENT TO NETWORK

To mitigate the risk to our network, our student information and employee information, MCC requires all devices being connected to our physical network to be reviewed and certified by the Information Technology Department (IT) prior to purchase and installation.

NETWORK ACCESS

1. Only MCC owned devices or devices owned by third parties that are necessary to aid in the functions of MCC, at MCC's request and approved by IT will be allowed on the physical MCC network.
2. Non-MCC devices will be allowed to access the wireless network. The wireless network will be setup with defined VLANs that are not on MCC's standard network. Access to any items on the MCC network will be controlled based upon the user ID and password used to connect to the wireless network.
3. Guest accounts may be requested for vendors and presenters needing temporary access to MCC's wireless network by calling the IT help desk.
4. Any devices that are connected to a physical network port by anyone other than IT will immediately be removed and confiscated.
5. Users wanting to connect a device to the MCC physical net-work:
    a. Must contact IT prior to the purchase of the device.
    b. IT will review the device and ensure that it will not compromise network security.
    c. Upon purchase of the device IT will install and connect the device to the network.

PHYSICAL ACCESS

The following shall be adhered to with respect to accessing Data Centers and Intermediate and Main Distribution Frame rooms (network closets):

1. Access shall only be granted by the IT department to MCC personnel and contractors to the extent their job or contractual responsibilities require access.
2. Lost or stolen access cards and/or keys must be reported without delay to MCCPD and Facilities.
3. Access by visitors or third parties must be tracked by a sign in sheet or electronic access control system. Visitors must be escorted by MCC personnel.

4. Access records must be reviewed periodically.
5. Signage for restricted access to rooms must be clearly displayed.

NETWORK DEVICE INVENTORY

IT will regularly inventory all devices connected to the physical MCC network. IT will be responsible for maintaining the inventory.

1. IT will regularly inventory all devices connected to the MCC physical network.
2. All devices connected to the physical network will be added to the IT Inventory system.
3. Any devices retired from service will be removed from the IT inventory system.
4. Any devices that are attached to the MCC network without the proper authorization will be disconnected and will not be allowed back on the physical network until the Device Attachment procedure has been followed.

NETWORK VULNERABILITY

In order to maintain a secure network, IT will perform Vulnerability Scanning and Penetration Testing of the MCC network.

SCANNING AND PENETRATION

1. MCC will have a qualified third party perform external penetration testing of the MCC network on a regular basis.
2. MCC will scan internal critical systems or those with heightened risk with frequent in-depth scans.
3. MCC will scan all other internal systems less frequently but at least once yearly.
4. Ad Hoc Scans will be performed prior to a new system being put into service and as needed in conjunction with a security incident.
5. High risk issues must be remediated in a timely manner.
6. Upon rectification of a vulnerability the system will be rescanned to ensure successful remediation.

REMOTE ACCESS

MCC recognizes the need for employees to have access to information while away from the district. MCC has a duty to protect the network to prevent unauthorized access and viruses from infiltrating the network. To support these needs, MCC has implemented remote desktop gateway and remote desktop access to allow approved access to the network without allowing any machine that is outside MCC's control from having a direct path to the network. This prevents viruses and external entities from harming our network.

Employee supervisors will be responsible for ensuring proper approvals have been obtained.