METROPOLITAN COMMUNITY COLLEGE

Security Guidelines for MCC's Network

MCC's network resources have become essential to MCC's ability to perform its mission as a public institution of higher education. These resources are critical to the delivery of instruction, to access to information and educational resources, to the provision of support services, and to communications and transactions among the institution and its various constituents. Therefore, providing for the effective security and management of MCC's network is a mission-critical function of the highest priority for the institution.

The following guidelines have been established to provide for the effective security and management of MCC's networked resources:

1. Only servers installed and managed by MCC's professional technical support staff will be allowed on MCC's network. No server software will be permitted to be installed on the MCC network by anyone other than MCC technical support staff. Any exception to this rule must be approved in writing by the vice chancellor for education and technology.

2. MCC will provide instructional course sites for all MCC courses on the MCC network. All such course sites will use a standard course management system software (currently Blackboard) selected by a districtwide committee of faculty and administrators and supported by the office of distance education services and MCC's technical help desk, Tech Line. No course sites using alternative software will be allowed on the MCC network.

3. As necessary, MCC technical support staff will make arrangements to support and host servers and web sites necessary to support specialized instruction that cannot be supported by the standard course management system. Such arrangements must be approved in writing by the vice chancellor for education and technology.

4. Laptop computers of vendors, service providers, students or other external clients will not be allowed to be connected to the MCC network except under the direct supervision of MCC professional technical support staff. Wireless access to the MCC network may be provided and managed by MCC technical support staff.

5. MCC will publish usage guidelines for computer labs available to students and to the general public. These guidelines will include rules regarding the connection of peripheral devices to lab computers, the downloading of software, and other practices that bear upon the security of the network, as well as policies regarding acceptable use of network resources.

6. MCC will support and host other public web sites that support the instructional, support and service missions of the institution. All such web sites will be required to comply with MoreNet policies, MCC acceptable use policies, noncommercial use, required content maintenance, appropriate logo use, ADA compliance, compliance with other fair use and educational standards, and other such standards or criteria that might be established by MCC. Sponsors of all public web sites on MCC's network must complete an application, receive approval, and seek renewal every two years.

7. Software deemed to have no legitimate purpose to support the missions and functions of the institution is prohibited from the MCC network. Prohibited software includes all network and application hacking tools, all illegal file sharing software, all personal web server software, and other software determined to be a threat to the security or health of the institution. MCC will publish and periodically update a list of specific examples of prohibited software, but this list will not restrict MCC's ability to ban other software judged to have no legitimate purpose on the network.

8. MCC retains the right to stop any illegal activity, including illegal file sharing, copyright infringement or criminal conduct, immediately upon discovery.