M|I|C/A

# INFRASTRUCTURE SECURITY POLICY

## I. POLICY

### A. GENERAL POLICY

1) Access to any network-connected computer must be via a logon process that identifies and authenticates the user, except where read-only access is given to certain systems (library catalog for example), or unprivileged access is normal and appropriate safeguards are in place (such as Web browsers in kiosk mode, or access to a contained web site).

2) No shared accounts will be created, except where absolutely necessary, and under the condition that a list is kept of the users of the account, and that they are jointly responsible for any action taken using the account.

3) Computers configured with the intent of accepting connections from other computers are considered to be servers, and must be physically located in one of the University's designated server rooms, providing suitable power protection, air handling, fire protections, physical security, and monitoring.

4) Only an authorized system administrator may alter a computer's network settings and parameters, and user access controls lists.

### B. OFFICE AND LAB COMPUTERS

In addition to the General Policy, the following policy applies specifically to computers physically located in an office or computer lab environment or designated for use as an office computer or workstation:

1) Users of an office or lab computer are responsible for all activity that originates from that computer while they are logged into it.

2) Users are responsible for all data they store on an office or lab computer. This includes the confidentiality of the data if it is sensitive, and the appropriate archival (backup) of the data if it has value.

3) Users are responsible for completing the logout process when finished using an office or lab computer. The logout process is often required to ensure that some data is properly saved back to a central computer server.

4) Users should never leave an office or lab computer unattended unless, they have either logged out, or the screen and keyboard have been locked using a password protected locking mechanism.

5) Office and lab computers may not be configured to accept connections from other computers, including, but not limited to, providing Internet services such as web and FTP servers, or to provide remote control of the computer.

6) Every stationary computer should have its own dedicated network jack, which should not be shared with other network devices, whether stationary or mobile.

7) Network hubs and switches may not be connected to office and lab network jacks. When these devices are detected attached to a network jack, the jack will be deactivated remotely without warning.

C. COMPUTER SERVERS

Computers configured with the whole or partial purpose of accepting connections from, and exchanging information between, other computers is

defined by this policy as a server. In addition to the General Policy, the following policies also apply to computer servers:

1) Servers must be physically secure. Physical access must be restricted to authorized system administrators only. Unauthorized users who require physical access to, or in the vicinity of a network server must be escorted by an authorized system administrator.

2) Servers must be located in an area that provides appropriate environmental controls, including air handling & conditioning, uninterruptible power protection (UPS) & conditioning, and fire suppression.

3) Servers must be appropriately managed and monitored on a daily basis by an authorized system administrator.

4) Reasonable attempts must be made to secure servers against published security vulnerabilities. This includes the timely application of patches, service packs, and hotfixes to vulnerable operating systems and applications, so long as the corrective action itself will not adversely affect the proper operation of the server

## D. NETWORK BACKBONE AND ASSOCIATED INFRASTRUCTURE

The College Network Backbone consists of the central network infrastructure, which connects and provides voice and data transport to all network connected computers and devices. The College Network Backbone also interconnects the College's independent network facilities, and provides access to Internet and intra-campus connectivity. The term Network Devices described below includes network hubs, switches, routers, PBX's, and all cabling, and termination hardware.

1) Appropriate access control will be configured and in place on all network devices with remote login capability.

2) Network devices will be located, wherever possible, within a suitable network or telecommunication closet, or in a designated server room.

3) Physical access to network and telecommunications closets must be restricted to authorized network and telecommunications personnel.

4) Network devices should be located in an area that provides appropriate environmental controls, including air handling & conditioning, uninterruptible power protection (UPS) & conditioning, and fire suppression.

## E. INDEPENDENT NETWORKS

Independent Networks are those networks connected to the College's Network Backbone and which Technology Systems and Services does not manage on a daily basis. These are networks for which TSS allocates network resources, supplies a connection to the College Network Backbone, and allows a College organization or entity to manage the network resources within that environment independent of TSS's daily operations. In addition to the General Policy, the following policies also apply to Independent Networks.

1) College organizations or entities hosting an independent network must designate a suitably qualified individual as the "Network Administrator" with responsibility for all network-connected devices within that network.

2) All software must be properly licensed. Licensing information must be readily available for audit. Licensing audits will be performed yearly, and on an as needed basis.

3) Adequate backup procedures must be in place.

4) Adequate virus protection software must be installed and frequently updated.

5) TSS will utilize firewalls and router Access Control Lists (ACLs) to limit the types of traffic that may enter and leave the College Network Backbone.

6) Dialup, wireless, and VPN technologies typically bypass university firewalls and access control lists. Such systems must be approved and registered with TSS before being attached to an independent network.

7) All network-connected devices must be monitored in order to detect breaches in security. In the event of any breach, Technology Systems and Services will be immediately alerted.

8) If TSS detects or is informed of a security threat or breach coming from within an Independent Network, and is unable to immediately reach the designated Network Administrator or a backup individual if supplied, TSS will disconnect that network from the College's Network Backbone.

9) All College organizations and entities hosting an independent network should have it's own Network Security Policy prominently displayed. Such policy will not supersede the MICA Infrastructure Security Policy.

F. AIRWAVES

The airwaves local to the College campus are considered a transmission medium and therefore a voice/data network resource. Since the airwaves are a shared resource, TSS is responsible for the management and allocation of bandwidth on this medium. In addition to the General Policy, the following policies also apply to the use of the College airwaves for voice & data transport. Wireless access points are defined for the policy below as being devices which serve as connection points between wireless technology and wired technology; this includes all forms of wireless networking hardware/software, wireless telephones, both Radio Frequency (RF) devices, and Infra-Red (IR) devices.

1) All wireless access points must be registered and pre-approved by TSS before being placed into service.

2) All wireless access points must be secured from unauthorized use. Appropriate forms of authentication and authorization will vary depending on the wireless medium.

G. DISASTER RECOVERY

1. To mitigate the impact of a local or total loss of network connectivity, and facilitate the quick recovery of network services in the event of a disaster, the College requires the following of all computing facilities:

1) All data considered "critical" to the operation of the College as a whole or to the services provided by a department, must be routinely backed up by the party responsible for that data, with archives being stored off-site at regular intervals.

2) Backed up data must be tested periodically to ensure that the media and restoration procedures are in working order, and that the data is in fact retrievable.

In addition, TSS specifically provides the following:

1) All servers managed by TSS are routinely backed up to tape, and the tapes stored in a building other than that where the servers are located. User data that is stored on any of the TSS supported network drives is backed-up automatically during this process.

2) All network devices necessary to the continued operation of College network services are maintained on a hardware support plan.

3) All network devices critical to the continued operation of College network services are configured in fault-tolerant designs or utilizing on-site spares wherever possible.

MARYLAND INSTITUTE COLLEGE OF ART

1300 MOUNT ROYAL AVENUE
BALTIMORE, MD 21217
T 410.669.9200
WWW.MICA.EDU