University of Baltimore

III-2.2 Network Security Policy

July 20, 2006
Reviewed on 8/1/2016

This document establishes the network security policy for the University of Baltimore.

The network security policy is intended to protect the integrity of the campus network and to mitigate the risks and losses associated with security threats to the campus network and network resources. The goals of this policy are to:

1. Safeguard the integrity and availability of the campus voice and data network.
2. Reduce threats to integrity and availability of computer systems connected to the network.
3. Reduce the likelihood that computers on campus are used to attack other organizations.

This policy will be posted on the University's web site. All revisions will be posted as they become approved.

The Chief Information Officer (CIO) will be responsible for actions pursuant to this policy.

I. General Policy

The following general policies apply to all computers connected to the campus network:

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 secured in a location that meets the University's standards and guidelines for servers.
4. Only an authorized system administrator may alter a computer's network settings and parameters, and user access controls lists.
5. Personal equipment may not be connected to the University network without the written authorization from the office of the Chief Information Officer.
6. 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.
7. Adequate backup procedures must be in place.
8. Adequate virus protection software must be installed and frequently updated.
9. Critical updates and patches must be routinely applied to computer operating systems and applications.

II. Office and Lab Computers

In addition to the General Policy, the following policy applies specifically to computers that are connected to the University Network and 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. Equipment borrowed(checked-out) from OTS by the member\group of UB community is intended to be used only by the member\group who borrowed it.
3. 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.
4. 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.
5. 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.
6. Office and lab computers, laptops, smartphones and tablets 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.

7. Computer devices must be connected to designated network wall or floor jacks. Each computer must be connected directly to an OTS managed and designated network jack, or through a UB IP telephone where appropriate, via a suitable network cable. Computer devices must be configured in a one device to one jack ratio. Sharing of the network jack among two or more computer devices is prohibited. Connecting personally owned computers and network equipment to university network jacks is prohibited.
8. Network hubs, switches, routers and Wi-Fi access points may not be connected to office and lab network jacks, unless approved by OTS. When these devices are detected attached to a network jack, the jack will be deactivated remotely without warning.

III. 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 hot fixes to vulnerable operating systems and applications, so long as the corrective action itself will not adversely affect the proper operation of the server.

IV. Campus Network Backbone and Associated Infrastructure

The Campus Network Backbone consists of the central network infrastructure, which connects and provides voice and data transport to all network connected computers and devices. The Campus Network Backbone also interconnects the University'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. If financially feasible, 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.

V. University Independent Networks

Independent Networks are those networks connected to the campus network backbone and which OTS does not manage on a daily basis . Such networks are generally specific purpose computing facilities, for which OTS allocates network resources, supplies a connection to the campus network backbone, and allows a university organization or entity to manage the network resources within that environment independent of OTS's daily operations. In addition to the General Policy, the following policies also apply to Independent Networks.

1. University 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, and for compliance with the policies below as well as all other applicable State and University IT polices and standards.
2. OTS will utilize firewalls and router Access Control Lists (ACLs) to limit the types of traffic that may enter and leave the Campus Network Backbone.
3. VPN, wireless, and dialup technologies typically bypass university firewalls and access control lists. Such systems must be approved and registered with OTS before being attached to an independent network.
4. All network-connected devices must be monitored in order to detect breaches in security, in accordance with established University standards and guidelines. In the event of any breach, the University Information Security Officer will be immediately alerted.
5. If OTS 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, OTS will disconnect that network from the University's Network Backbone.
6. Each University organization or entity hosting an independent network should have the University of Baltimore's Network Security Policy prominently displayed, or referenced (via hyperlink for example), in addition to any local network policies, as necessary. Local network security policies may not supersede the University of Baltimore's Network Security Policy.

VI. University Airwaves

The airwaves local to the University campus are considered a transmission medium and therefore a voice/data network resource. Since the airwaves are a shared resource, OTS 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 University 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 OTS 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.

VII. Disaster Recovery

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 University requires the following of all computing facilities:

1. All data considered “critical” to the operation of the University 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.

For more information, please refer to OTS Disaster Recovery Plan.