Mid-Atlantic Christian University
Office of Information Technology Policy #3

SUBJECT: Network Infrastructure

DATE: April 08, 2013

REVISED: 02/11/2014; 02/27/2015; April 2020
NEXT SCHEDULED REVIEW: Yearly, February

APPROVED BY BOARD OF TRUSTEES: October 18, 2013

Policy for: All divisions of Mid-Atlantic Christian University
Procedure for: All divisions of Mid-Atlantic Christian University
Authorized by: Vice-president for Finance
Issued by: Board of Trustees

I. Purpose

The purpose is to assign responsibility for all aspects of creating, using, integrating, designing, installing, managing and maintaining the University's Network Infrastructure and its Core Network Services.

II. Policy

The Office of Information Technology ("OIT") centrally maintains Mid-Atlantic Christian University's ("University") network infrastructure. OIT is responsible for the installation, management, support, and providing access to the University network.

Auxiliary Systems that utilize the University network, or building wiring, or co-locate with campus network facilities, or electronics must be developed, installed, and operated in cooperation and/or coordination with OIT oversight. OIT or software owner will maintain practices regarding the operation of each specific system.

III. Procedures

A. Network Identity
   1. *Global naming and addressing* – OIT is responsible for providing a consistent forum for the identification and allocation of Internet Protocol (IP) addressing and naming conventions. Dynamic Host Configuration Protocol (DHCP) is the preferred method for the assignment of IP addresses. Exceptions to DHCP address assignment must be requested from OIT.

2. *Responsibility* – OIT is responsible for the standards, design, implementation, performance and operation of the University Network Infrastructure. OIT is responsible for monitoring compliance with this policy, within the scope of Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use.

B. Access

1. *Access* – Access to the Network Infrastructure is provided to University faculty, staff, students, affiliates and guests, in a classification labeled "Authorized Users".

2. *Authentication* – Wireless Network interfaces and computing devices requires user authentication to access the Wireless Network. Implementing network access with the intent to bypass authentication is a violation of this policy and a violation of the Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use.

3. *Authorization* – Network users are authorized through their network access to utilize specific Resources based on need. Access to educational and research resources is supported with open authorized access. Access to administrative and business operations requires specific "need to know" attached to job requirements, and requires approval by an appropriate vice president. Network authorization will not define or create access where no need exists. Network authorization tools and strategies will implement and support the rules, guidelines and strategies defined by the Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use and network resource owners.

4. *Devices connecting to the network* – OIT maintains a list of acceptable devices and supported devices, including devices identified in the Desktop Service Level Agreement. Functionality of any other device is the responsibility of the owner. Any device (wired or wireless) connected to the network is subject to all university policies, particularly the Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use, regardless of ownership.

5. *Third Party/Backdoor Attachments* – Attachments to the network by non-university organizations or network users must be approved by OIT and adhere to Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use.

C. General Usage and Connectivity Guidelines

1. *Network Usage and connectivity* – Use of the Network Infrastructure must be in a manner consistent with the Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use . Equipment or network activity that violates this Network Policy will be subject to the disciplinary actions as outlined in the Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use, which may include disconnecting or blocking such equipment or network activity.

2. *Addressing* – MAC and IP Addresses must be standardized in use and not altered or fraudulently presented. Alteration of addressing information is a violation of this policy and subject to sanction.

3. *Planning* – OIT must be involved in initial and ongoing planning and budgeting for all aspects of the University Network Infrastructure in existing structures, renovations, new structures, and remodeled areas including planning for connectivity of the University Network Infrastructure to remote of off-campus locations.

4. *Compliance* – Network Components, Wired Network, and Wireless Network installations and implementations will be monitored for conformance to established University Network Infrastructure plans, as well as, regulatory compliance and industry best practices.

5. *Contracted network support* – OIT must pre-approve all contracted vendor work on the University Network Infrastructure. All contracted vendor support work will be monitored for compliance to current University technical standards, quality installation, and work completion in a timely manner. OIT may also choose to centrally sub-contract some operational and engineering network functions. Departments will be assessed for the work and project management cost of tasks that require contracted network support.

6. *Installation and removal of Network Components and Access Points* – OIT must authorize the installation and/or removal of Network Components and Access Points prior to any work. Tampering with, altering, or moving Network Components or Access Points is prohibited unless prior approval is obtained through OIT. The location of all wireless Access Points must be coordinated with existing OIT plans.

7. *Remote access services* – Acceptable remote access to the Network Infrastructure, such as virtual private network is defined and maintained by OIT. OIT will seek to provide the most secure remote access connection appropriate to the security requirements defined by the affected network resource owners and managers. All external connections to the university network must first be reviewed and approved by OIT.

D. Additional Wireless Guidelines

1. *Wireless Network legal restrictions* – The special nature of Wireless Networks may be subject to legal restriction. Wireless Access Points must abide by all federal, state, and local laws pertaining to Wireless Networks. OIT is responsible for review of current technologies and legal restrictions. OIT will authorize the installation or design of wireless access with full consideration to this limitation.

2. *Interference resolution* – Certain wireless devices exist that utilize the same wireless frequency as the data network. In the event that a wireless device interferes with

other equipment, OIT shall work with key representatives of units and departments in the coverage area to seek resolution.

3. *Wireless Network cards* – Wireless Network cards are to be configured in client only mode and are not to be used as bridges, base stations, Access Points, or as an ad hoc network.

4. *Wireless Availability* **-** Wireless access is available in the following locations:

    i. Pearl A. Presley Hall
    ii. Heritage Hall
    iii. Student Life Center
    iv. Albert C. Blanton III Campus Life Center
    v. Wilkinson Hall
    vi. Faith Hall
    vii. The Welcome Center

    Only the IEEE 802.11g and/or 802.11n standard for WLANs will be supported.

5. Resource Provisioning

    1. Provisioning of Staff and Faculty Computers **-** Staff and faculty should make an appropriate request for information technology resources through their department vice president. Staff and faculty have the option of using a University-owned desktop or laptop.

    2. Provisioning of Student Computers **-** Student computers are not provided by the University. Students are expected to provide for their personal computing needs.

IV. Published

V. Reasons for Revision

VI. Appendices

Definitions	
Auxiliary Services	s Campus cable TV, fire alarm systems, automation or control systems, alarm systems, AV systems, surveillance cameras, or any other networked electronic or computer system

Relevant Policies

Office of Information Technology Policy #1 F-IT 01 -- Acceptable Use