University of Baltimore

III-2.3 Wireless Network Policy

Revised and approved by President Bogomolny 11/16/2010 to reflect current wireless network configuration and to meet USM requirements.
Reviewed on 8/1/2016

I. Purpose

This document provides policies, standards, and guidelines for best practices as they relate to providing and using the University of Baltimore wireless networks.

II. Overview

Wireless networking is an extension of the University's existing wired network infrastructure. It allows wireless enabled and mobile device users to access university network resources and the public Internet. The University provides multiple levels of wireless access services that offer either unencrypted or encrypted overthe-air security.

III. Security and Access

Wireless transmissions over the University's services that are not encrypted should not be relied upon as being secure. It is the responsibility of the user to ensure that communications which include the transmission of personal or sensitive data is encrypted utilizing a secure protocol such as SSL (https). Data protection is the responsibility of the application and data owners. Users are responsible for protecting data on personal devices.

The University's encrypted wireless services secure local over-the-air transmission, but should not be relied upon as providing a completely secure communication path. It is the responsibility of the user to ensure that communications which include the transmission of personal or sensitive data is also encrypted utilizing a secure protocol such as SSL (https). Data protection is the responsibility of the application and data owners. Users are responsible for protecting data on personal devices.

The University's wireless services and supported security protocols may be found at http://www.ubalt.edu/wireless.

Authentication. Wireless users must login to either service using a valid University NetID and password. After three successive authentication failures, all the wireless accounts, with an exception of Guest account, are automatically blacklisted from wireless access for 5 minutes. After the five minute period has elapsed, the account is automatically de-blacklisted.

Access Limitations. Authenticated wireless clients will have access to outbound Internet services, including MyUB and access to web based email services. Shared network storage is not available to wireless clients, except as available through the MyUB portal.

IP Addressing. DHCP (Dynamic Host Configuration Protocol) will be used.

Wireless Protocols. The University of Baltimore provides wireless access using the 802.11a/b/g/n protocols. Only the 802.11b/g protocols are supported on the crowded 2.4Ghz band, while 802.11a/n are supported on the 5 Ghz band.

IV. Support

Personal device purchases, compatibility, configuration, installation, setup, security, and utilization of the wireless network are the responsibility of the user.

Support is limited to the network infrastructure and network user accounts. Suspected network problems and issues pertaining to network accounts should be directed to the OTS Call Center (410) 837-6262.

V. Users

Equipment. Users are responsible for purchasing and/or providing compatible and appropriately configured client devices and wireless 802.11 network interfaces.

Network Account. Users are responsible for obtaining a valid University network account (NetID) and password. All wireless access is authenticated. Access is available only to University of Baltimore faculty, staff and students. Special accommodations for guests are permitted through select offices on campus.

VI. Related Policy References

1. Code of Conduct
2. Acceptable Use of Information Technology Resources
3. E-mail Policy
4. E-mail Guidelines
5. Network Security Policy
6. Information Technology Security Policy