

# University of Maryland Baltimore (UMB) Wireless Security Standard

Effective Date: 04/14/03

## **Purpose**

This standard establishes a framework for ensuring that wireless networking technologies deployed within the University of Maryland's campus are managed in a secure fashion.

Wireless network systems are vulnerable to hacking and break-ins. It is UMB's responsibility to protect and maintain the security of the networks we are charged with managing. As administrators, we are obliged to prevent trespassers from corrupting or misusing the campus network. Listed below are security standards that are recommended to be followed where technically feasible.

## **Background**

UMB is a distributed environment with corresponding local responsibilities for wireless network systems. It is recommended that wireless systems be installed using the campus de facto standard for networking infrastructure e.g., Cisco switches and firewalls. The security model proposed makes assumptions on the use of Cisco switches and firewalls to make the wireless network as secure as possible. It will be the local network administrator's responsibility for identifying and authenticating wireless users requiring access. As the campus Directory Services project progresses, central authentication of users should be possible from any wireless network across the campus.

## **Scope**

This security standard applies to all wireless network resources and all users who access those resources. It pertains especially to those resources that support vital business functions and that maintain confidential, sensitive, private, personal or institutional information.

## **Standard(s)**

To maximize the security of the wireless network segment:

- Maintain physical access controls
- Maintain a separate VLAN for wireless connections on building switch
- All Access Points within the building to be contained in wireless VLAN

## **Standard(s) continued**

- Do not place any servers or services on the wireless network, it should only be used for

wireless workstation connections

- DHCP server to provide wireless connections with a non-routable IP Addresses
- VPN server to provide a routable IP address only after authenticating the user to your local database or campus-wide Directory Services
- Establish local security policies for distributing VPN clients to authorized users
- Ensure that antivirus software and a personal firewall are installed on clients connected via wireless technology

To ensure a properly installed wireless network:

- Obtain a site survey from a qualified contractor to enable maximum coverage without having large areas of wireless connectivity outside of the building
- Use only 802.11 products with viable long-term security strategies and longevity, e.g., Cisco