

# Messiah College Wireless Communication Policy

## I. Purpose

This policy prohibits access to Messiah College networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Technology Services (ITS) are approved for connectivity to Messiah College's networks.

## II. Policy

### A. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDA's, etc.) connected to any of Messiah College's internal networks. This includes any form of wireless communication device capable of transmitting packet data.

### B. Approved Technology

All wireless LAN access must use ITS approved vendor products and security configurations. Non-ITS approved access points are not allowed to be installed unless an exception is granted by ITS.

### C. Encryption and Authentication

ITS requires authentication to all campus wireless networks and strongly suggests encryption. Limited network resources be granted to none encrypted hardware.

## III. Additional Policy References

### A. Messiah College Computing Access Policy

This policy applies to anyone who uses the college's computers and networks and articulates the standards of behavior that are expected of all users. The college retains its legal ownership and right to use information residing or transmitted on college owned systems. With this policy, the college does not restrict in any way its legal right to monitor and control computing activity occurring on college owned systems and networks. The Chief Information Officer (CIO) is responsible to carry out this policy, and to make referrals to appropriate administrative offices when necessary. Any exception to this policy must be approved by the CIO.

### B. Messiah College Guest Account Access Policy

Typically, only Messiah College faculty, staff, and students are eligible for network accounts. There are specific circumstances that require others to be eligible for an account as a guest and therefore be given access to a guest account. Therefore, in order to retain our status as a private network, to ensure compliance with Communications

Assistance for Law Enforcement Act (CALEA), and to prevent unrestricted access to the network by unauthorized individuals we require all Messiah College guests who require network access use a guest account.

**C. Messiah College Remote Access Policy**

The purpose of this policy is to define standards for connecting to Messiah College's network from any host. These standards are designed to minimize the potential exposure to the college from damages which may result from unauthorized use of college resources. Damages include the loss of sensitive or college confidential data, intellectual property, damage to public image, damage to critical internal systems, and other damage deemed critical by Information Technology Services (ITS).

**IV. Enforcement**

Anyone not complying with the standards set forth will be referred to the appropriate campus and/or external authority.