Title: Wireless Access and Usage Policy

Policy Purpose: The purpose of this policy is to ensure that enabling a wireless infrastructure at Emory does not create security holes that could potentially threaten the confidentiality, integrity and availability to electronic protected health information (ePHI), or any information system containing sensitive business, financial or other confidential information.

Requirements:

1. All network communication devices which provide for simultaneous access by more than one Ethernet device, including wireless Access Points/Base Stations connected to the Emory network, must be approved by University Technology Services and Information Security.
   a. Unauthorized network communication devices are subject to disconnection from Emory networks without warning or notice.
2. Devices that are network intrusive (i.e. devices that monitor network communications, interrupt network services, or change the network topology of the Emory network in any way) are prohibited without approval of University Technology Services. Such devices include, but are not limited to hubs, switches, port splitters, routers, wireless access points, multi-homed PC’s, and packet/data monitoring equipment or software.
3. Network communication services and wiring must not be modified or extended beyond their area of intended use. This applies to all network wiring, hardware, and jacks.
4. All wireless access points connected to Emory networks must be deployed, configured, maintained, and managed by University Technology Services. Any exceptions to this requirement must be authorized by University Technology Services.
5. All wireless access points connected to the Emory network must comply with the following requirements.
   a. Access points must be enterprise class devices.
   b. The hardware address (MAC) of all access points must be registered with University Technology Services.
   c. Access points must be configured in accordance with University Technology Services configuration standards.
   d. Access points must utilize only the IP addresses, network ports, and SSIDs assigned by University Technology Services.
Access points must utilize WPA or WPA2 security. Access points utilizing no encryption or WEP encryption are prohibited unless explicitly approved by University Technology Services and Information Security teams.

Local administrative accounts for all access points must have complex passwords that expire every 365 days (see Password Management Policy).

Physical security of the access points should be considered during initial design/site surveys and maintained after implementation. Whenever feasible, access points should be:

- located in physically secured areas
- located out of sight
- protected against tampering and theft

Wireless access points are subject to periodic penetration testing and audits without prior notice.

Wireless clients connected to the Emory network must comply with the following requirements:

- Wireless clients must be protected by a host based firewall.
- Wireless clients must utilize anti-virus software that is up to date and has current anti-virus signatures.
- Wireless clients must be kept up to date with the latest operating system and application security patches.
- Wireless clients must not be connected to both wireless and wired Emory networks simultaneously.
- Wireless clients must be configured so they will not automatically connect to ad-hoc or unsecured wireless networks.

Users are prohibited from accessing Emory networks via unsecured wireless communication mechanisms or through an unregistered/unapproved device. Only devices that meet the criteria of this policy or have been granted an exclusive waiver by the HIPAA Steering Committee or delegates of the committee are approved for connectivity to Emory networks.

Anyone accessing the Emory wireless network must comply with all applicable policies governing the appropriate usage of computers, communications and all other policies relevant to the security of Emory information systems.

This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

See: HIPAA Security Regulations: Sanction Policy

Recommended By: Emory HIPAA Security Working Group
Effective Date: April 20, 2005
Authorized By: Emory HIPAA Security Steering Committee
Date of Last Edit: April 21, 2011
Review Date: April 21, 2011