Wireless Network Security Standard

Periodic reports are run and exhibit Active Interfering AP’s and Rogue AP’s on the Business School wireless network. Interfering AP’s can compromise our signal strength and hence service to our community. Rogue AP’s can be a serious threat to security. The following are steps which will be taken.

Connectivity

The Goizueta Business School wireless network is part of the Emory University wireless network. Hence you can seamlessly navigate throughout campus without having to reconnect.

You may connect to one of two SSID’s via the wireless network at Goizueta:

**EmoryUnplugged** - Emory Unplugged is the preferred WPA wireless service for the Emory community. To connect, either follow the instructions below or download the automatic configuration script from the Software Express service at [software.emory.edu/express](http://software.emory.edu/express)

**EmoryGuest** - EmoryGuest is an unsecured wireless network that only gives you access to the Internet. You cannot access the First Class client or print using EmoryGuest. EmoryGuest is restricted in the following manner:

- Network bandwidth will be throttled to 0.5Mb per second.
- Each session will expire in four hours.
- Access is restricted to http and https protocols, though users may use VPN to "tunnel" to their home networks.
- Access may be restricted to other Emory resources that allow usage only by Emory students, faculty, and staff. These may include library databases and certain networked applications, among others.

Note: EmoryGuest is provided without encryption, therefore users access this wireless network at their own risk.

Acceptable Use – The wireless network is a shared resource. The wireless network is not meant to be used where intensive throughput is involved. The uploading/downloading of large files, video and audio is inappropriate use of the wireless network.