American
Jewish
University

WIRELESS NETWORK POLICY

This is a deployment guide for wireless networking at the American Jewish University to ensure reliable, compatible, and secure operations. By virtue of using the wireless network, the user agrees to be bound by this policy. This policy will be posted on the University's website

- AJU Campus Technology Department will be the sole provider of design, specification, installation, operation, maintenance, and management services for all wireless Access Points.
- Wireless network users may not install or operate WLAN (Wireless Local Area Network) Access Points on the university's property.
- AJU is responsible for the Access Point and the wired network to which it is attached.
- Individual users will be responsible for all costs associated with purchase, installation, operation, and support of wireless adapters in client computers.
- Residence Life Complex: The wireless network was tested and designed to serve the dorm buildings only. Apartment residents who choose to use the network services, do so on their own responsibility. Reception rates in different dorm rooms will not be considered by the RLO when assigning rooms to residents.
- To ensure an efficient use of the wireless network, the University may block certain ports and protocols. This includes but is not limited to: certain online services, IM and file sharing.
- Network connections are a shared resource. Users should ensure their network use does not generate an inordinate amount of traffic or adversely affect others. While Web browsers and sending/receiving electronic mail seldom cause problems, users who use services such as file transfer protocol (ftp) sites should ensure their systems do not adversely affect the entire network.

Wireless network users shall:

a) Respect the integrity of the University computer systems and network.
b) Respect the privacy of other computer users.
c) Respect the rules, regulation and procedures governing in Wireless Network Policy.

Unacceptable uses - you may not perform these activities:

a) Examine, alter, or attempt to examine/alter another computer user's private files or electronic communications without authorization;
b) harass or interfere with other University computer users;
c) use software that overloads the network;
d) connect unauthorized electronic equipment to the network;
e) connect equipment to the network in an unauthorized fashion;
f) knowingly transmit viruses.

Non-Confidentiality:

The University recognizes that users might believe computer files and e-mail messages are confidential; however, such files and messages are subject to the access by Computer Services of user's files at systems maintenance times as well as when there is a report of suspected unlawful or improper activities. User's files are not confidential. The University reserves the right to review all information on any University server or network.

Security and Privacy:

It is important to notice that while using network services the information on the user's computer is exposed to the rest of other network users. The AJU will not be responsible for any damage for personal computer/files or for violation of privacy rights conducted by other users. Each user will be responsible to protect and secure his personal computer and data.

The use of the university's wireless network is a privilege, not a right. The AJU may protect legitimate facilities users by imposing sanctions on users who abuse this privilege.

Improper use of the wireless network or on purpose damage to the wireless network will result in temporary or permanent discontinuance of wireless network services by the AJU. In this case, the AJU will have no responsibility to compensate users for network adapters they purchased.