

Wireless Security Requirements

Improperly secured wireless access points can compromise the security and performance of the University network, providing easy access for intruders to steal passwords, destroy data, and use University network and Internet resources for unauthorized purposes. Any department that deploys wireless networking devices must, at a minimum, follow these basic security practices:

- ❑ Reasonable measures must be taken to ensure that wireless access points, their power supplies, and other associated equipment are protected from physical access by unauthorized persons.
- ❑ The default administrative password for a wireless access point shall be changed to a non-trivial string.
- ❑ Wireless networks should not be used to access critical data or systems (e.g. root shells on servers, administrative functions on web servers, etc.) unless additional security is used such as a VPN, SSL, or SSH client.
- ❑ Encryption should be enabled on all wireless access points. Encryption provides a minimal level of protection only, and should not be relied upon as protection against intrusion or data theft.
- ❑ Departmental access points, i.e. other than public access points deployed by ITU, should be configured to disable "broadcast SSID" if this function is supported on the equipment. This requirement is needed to prevent interference with public access points deployed by ITU.
- ❑ Access points must be configured to deny connections from unauthorized users, either by restricting connections to specific hardware (MAC) addresses, or through other means approved by ITU Network Engineering and Technology.