

	Information and Communications Technology Division	Policy	
		Effective Date	Date of Last Revision
		September 1, 2005	September 1, 2005

Chapter Name	
6.0 NETWORKING	
Chapter Number	Title
6.2	Wireless Communication Policy

1.0 Purpose

This policy prohibits access to Eastern Michigan University (EMU) networks via unsecured wireless communication mechanisms. Only a wireless system that meets the criteria of this policy or has been granted an exclusive waiver by the Director IT, Network and Systems is approved for connectivity to EMU's networks.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, or other electronic devices of any nature) connected to any of EMU's internal networks, or (in some cases) residing on EMU property. This includes any form of wireless communication device capable of transmitting packet data.

In cases where policies conflict with each other, the most restrictive rule will always apply, unless explicitly stated otherwise.

This policy covers all wireless devices. Previously existing connections will not be grandfathered unless a waiver explaining why compliance is impossible and outlining a migration plan is approved by the Director of IT Security Administration and Director IT, Network and Systems. No waiver may be granted or extended beyond three months of this policy's approval.

3.0 Policy

Devices connected to the EMU network must follow all of the guidelines below. Devices not connected to the EMU network but resident on EMU property must not interfere with EMU wireless networks. If such a device does interfere with an EMU wireless network, this condition must be eliminated or the device must be disconnected.

1. Devices must adhere to current ICT standards. These standards are subject to change on short notice, or without notice if a security threat arises.
2. ICT maintains an official wireless network distributed over the entire campus. Wireless devices must not interfere with this network, or they will be disconnected. The official wireless network is configured with a user authentication system suitable for public use, and is the only network approved to offer public use (e.g. use by something other than an explicit list of immediately identifiable devices/users).
3. All wireless Access Points / Base Stations connected to the university network must be registered and approved by the Network Engineering team. These Access Points / Base Stations are subject to periodic penetration tests and audits.
4. All wireless LAN access must use ICT-approved vendor products and security configurations. Please consult the Director of Networking and Systems for the current configurations.
5. All wireless LANs must be configured to drop all unauthenticated and unencrypted traffic. Wireless implementations must maintain point to point hardware encryption compliant to current ICT standards. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address, which must be tied to identification of a single person with registered, accurate contact information. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar (these examples do not imply approval).

6. When possible, the SSID should not broadcast the name to reduce possible unauthorized connections.
7. When a wireless network is connected to the EMU network, users must understand that their machines are a de facto extension of EMU's network, and as such are subject to the same rules and regulations that apply to EMU-owned equipment, i.e., their machines must be configured to comply with all EMU security policies. Unless officially a member of the public network, devices connected over wireless to EMU are also considered part of the non-public network. More details can be found in the *Secure Network Devices Policy* and the *Acceptable Use Policy*.

4.0 Responsibility for Implementation

Director of IT Security Administration and Director IT, Network and Systems.

5.0 Enforcement

Any user found to have violated this policy may be subject to loss of certain privileges or services, and other disciplinary actions or legal sanctions, civil and criminal.

6.0 Definitions

<u>Term</u>	<u>Definition</u>
Access Point / Base Station	A piece of network equipment capable of relaying network traffic between wireless devices, or between wireless and wired devices.
LAN	A local area network is a computer network covering a certain area.
MAC address	A media access control address is a unique identifier attached to most network equipment.
PDA	A personal digital assistant is a type of portable computer.
RADIUS	Remote authentication dial-in user service is a protocol for identifying, authorizing, and accounting network users.
SSID	A service set identifier is a code attached to all packets of a wireless network identifying those packets as part of that network. Packets must contain this ID to communicate on that network.
TACACS+	Terminal access controller access control system (plus) is a protocol for identifying, authorizing, and accounting network users.
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

7.0 Revision History

<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
ICT Security	Modeled after SANS Institute Policy		
ICT Security	ICT Security Team	May 17, 2005	
Barr	Revised	June 20, 2005	
French	Revised	June 21, 2005	
Popp	Submitted to CIO	July 28, 2005	September 1, 2005
Laundra	Copyedited/proofed for upload	September 1, 2005	