

Chapter Name

6.0 NETWORKING

Chapter Number Title

6.3 Open Area Network Security Policy

1.0 Purpose

This purpose of this policy is to outline restrictions imposed on Eastern Michigan University (EMU) open area networks (defined below) to reduce the risk of interruption of services, loss of sensitive or university data, intellectual property, damage to public image, damage to critical EMU internal systems, as well as any other damages which may be suffered by the University, or members of the University community including students, independent contractors, agents, and employees.

2.0 Scope

This policy applies to any EMU open area network, which is a network offering access to a changing or undefined set of users. This includes but is not limited to all EMU classrooms, labs, publicly accessible wireless environments, publicly accessible network outlets, and kiosks.

In cases where policies conflict with each other, the most restrictive rule will always apply, unless explicitly stated otherwise. This policy is not the sole governing policy for open area networks; other policies apply, including but not limited to the Secured Network Devices and Secure Network Equipment policies.

This policy covers all connected devices. No previously existing environments or arrangements will be grandfathered.

3.0 Policy

It is the responsibility of anyone planning, hosting or maintaining an open area network (hereafter referred to as open area operators) at EMU to contact the Director IT, Network and Systems or Assistance Director IT, Network and Systems to make them aware that an open area network is in place. If a written notice is not provided, the open area operator is in violation of this policy.

It is the responsibility of Division of Information Technology (DoIT) Network Engineering to maintain standard network security restrictions on all open area networks appropriate for ensuring the secure operation of the campus network. This responsibility does not release open area operators from the additional responsibilities imposed by any other applicable policy.

Open area environments shall comply with anti-virus, encryption, password, and other applicable workstation policies.

Including but not limited to:

1. Open areas must reside outside of the university firewall or impose restrictions identical to that arrangement, with some documented allowances for academic and business needs, provided secure communication and monitoring can be ensured.
2. Open areas must employ a secure authentication system to identify all users in real-time and historically. This authentication system must be approved by DoIT Network Engineering and may be subject to additional requirements by other policies. Any exception to authentication required for device operation must be documented and coordinated with DoIT Network Engineering.

3. Accurate contact information for open area operators must be on-file with DoIT for any open area network.
4. Remote administration of equipment in open areas is expressly prohibited except when permitted in writing by DoIT Network Engineering.

DoIT reserves the right to disconnect or impose network limits on any open area network in the interests of performance, security, or academic/business needs.

4.0 Responsibility for Implementation

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

5.0 Enforcement

Enforcement will be handled by the Director of IT Security Administration and Director IT, Network and Systems.

Any user found to have violated this policy may be subject to loss of certain privileges or services. Disciplinary actions or legal sanctions, civil and criminal apply where stated by policy or law.

6.0 Definitions

<u>Term</u>	<u>Definition</u>
DoIT [In this document IT is synonymous with DoIT]	Division of Information Technology –[This is the new name for the Division of Information and Communications Technology.]
Open Area	Any area supplying network access to a changing or undefined set of users
Remote Administration	Network-based connections with privileged access from sources external to the open area

7.0 Revision History

<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
ICT Security	ICT Security Team		
Popp	Edits per PRC	April 26, 2007	
A. Barr	Revision of Policy number due to conflict	2-25-2008	
A. Barr	Edit using new template format; edit changes of ICT to Division of Information Technology (DoIT) Confirm final number and send to R. Winterhalter for meeting with College Techs. on 03-13-2008;	03-11-2008	
A. Barr	Prepare PDF version for posting to Web as proposed.	03-13-2008	