

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

Chapter Name	
8.0 SECURITY	
Chapter Number	Title
8.3	Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connections to any Eastern Michigan University (EMU) network or device from any external source. These standards are designed to minimize the potential exposure to EMU from damages which may result from unauthorized use of EMU resources. Damages include the 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 persons communicating with, working for or affiliated with Eastern Michigan University, including without limitation all EMU students, alumni, employees, contractors, vendors and agents with an EMU-owned or personally-owned computer or workstation used to connect to the EMU network. For example, this policy applies to remote access connections used to do work on behalf of EMU, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, and any other technology.

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

This policy covers all types of remote access. 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 one year of this policy's approval.

3.0 Policy

General

1. It is the responsibility of all persons connecting remotely to EMU's university network to ensure that their remote access connection is given the same consideration as an on-site connection to EMU.
2. General access to the Internet for recreational use by immediate household members through the EMU Network on personal computers is permitted for employees as allowed in the Acceptable Use Policy. The EMU employee is responsible to ensure the family member does not violate any EMU policies, does not perform illegal activities, and does not use the access for outside business interests. The EMU employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the university network via remote access methods, and acceptable use of EMU's network:
 - a. *Acceptable Encryption Policy*
 - b. *Virtual Private Network (VPN) Policy*
 - c. *Secure Network Devices Policy*

- d. *Wireless Communications Policy*
- e. *Acceptable Use Policy*

Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via strong password authentication or public/private keys with strong passwords. For information on creating a strong password see the *Password Policy*.
2. At no time should any person provide their login or email password to anyone; this includes co-workers and family members.
3. All persons connecting remotely must ensure that their EMU-owned or personal computer or workstation – when connected remotely to EMU’s university network – is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user. Complete control over a network implies not only that all aspects of the network can be managed by the user, but also that the user is aware of and can instantly identify all persons and devices using that network.
4. All persons connecting remotely must not use non-EMU email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct EMU business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a remote user’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Non-standard hardware and security configurations must be approved by Network Engineering and the Director of IT Security Administration before use.
7. All hosts connecting remotely must use the most up-to-date anti-virus software (<http://www.emich.edu/public/it/helpdesk/>), this includes personal computers.
8. Personal equipment that is used to connect to EMU’s networks must meet the requirements of EMU-owned equipment for remote access.
9. Organizations or individuals who wish to implement non-standard remote access solutions to the EMU production network must obtain prior approval from Network Engineering and Director of IT Security Administration. This approval must be written and on-file with Network Engineering, and may be revoked at any time.
10. In the interests of network security performance, EMU Network Engineering may disconnect network connections or services at any time if necessary.

4.0 Responsibility for Implementation

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

5.0 Enforcement

Any user found to have violated this policy may be subject to loss of certain privileges or services but not necessarily limited to the loss of remote access services, and other disciplinary actions or legal sanctions, civil and criminal.

6.0 Definitions

<u>Term</u>	<u>Definition</u>
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name “modem” for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the University network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a EMU-provided Remote Access home network, and connecting to another network, such as a spouse’s remote access. Configuring an ISDN router to dial into EMU and an ISP, depending on packet destination.

DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone university network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
SSH	Secure Shell: an encrypted remote connection standard.
VPN	Virtual Private Network: an encrypted, private network connection.

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	