

	<b>Information and Communications Technology Division</b>	<b>Policy</b>	
		<b>Effective Date</b>	<b>Date of Last Revision</b>
		September 1, 2005	September 1, 2005

<b>Chapter Name</b>	
<b>8.0 SECURITY</b>	
<b>Chapter Number</b>	<b>Title</b>
<b>8.4</b>	<b>VPN Connections Policy</b>

### 1.0 Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to or from Eastern Michigan University (EMU) networks.

### 2.0 Scope

This policy applies to all persons utilizing VPN connections to access EMU networks or access an external network from EMU networks.

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

This policy covers all VPN connections. 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 employees with VPN privileges to ensure that unauthorized users are not allowed access to EMU internal networks.
2. VPN use is to be controlled using strong passwords without storing the password locally on the machine. For information on creating a strong password see the *Password Policy*.
3. While connected, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. All computers communicating to or from EMU networks via VPN or any other technology must use the most up-to-date anti-virus software that is the university standard (<http://www.emich.edu/public/it/helpdesk/>); this includes personal computers.
6. All persons, including users of computers that are not EMU owned equipment must configure the equipment to comply with EMU's VPN, Remote Access, and any other applicable network policies. These requirements may be changed at any time by the EMU Network Engineering team.
7. By using VPN technology with personal equipment, 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. Devices connected over a VPN to or from 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*.

## VPN connections from campus

1. VPN Connections made from EMU networks to external networks will be required to maintain compliance with ICT standards in addition to this policy.
2. Any VPN connection may be disconnected by ICT for any reason, for any length of time including permanently.

## VPN connections to campus

Approved EMU employees and authorized third parties (customers, vendors, etc.) may connect to campus using a VPN, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Connections not directed through approved concentrators are not permitted (see below). ICT's VPN concentrator is designed to provide secure, encrypted access to resources on campus not normally available to off-campus users. Using the VPN concentrator to access off-campus resources (making EMU a proxy) is not permitted.

1. Access Control Lists (ACL) will be applied to every VPN connection explicitly defining the traffic allowed. These ACLs will be managed by the EMU Network Engineering team, and may change at any time.
2. VPN gateways must be set up and managed by the EMU Network Engineering team. VPN connections not approved and managed by the Network Engineering team are not permitted.
3. VPN users will be automatically disconnected from EMU's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Automated traffic generation (such as pings) are not to be used to keep the connection open.
4. The VPN concentrator is limited to an absolute connection time of 24 hours.
5. Only EMU-provided VPN clients may be used.
6. Applicants for VPN access must attend a technical training session prior to being granted access, or as otherwise approved by the Director of IT, Network and Systems.

## 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 but not necessarily limited to the loss of VPN services, and other disciplinary actions or legal sanctions, civil and criminal.

## 6.0 Definitions

<u>Term</u>	<u>Definition</u>
ACL	Access Control List: network security restrictions used to explicitly allow or deny traffic.
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	