EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

# Policy

| Effective Date | Date of Last Revision |
|---|---|
| September 1, 2005 | January 27, 2014 |

| Chapter Name | |
|---|---|
| Security | |
| **Chapter Number** | **Title** |
| **8.4** | **VPN Connection Policy** |

## 1.0 Purpose

The purpose of this policy is to guide university employees in the appropriate use of 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 to access an external VPN from EMU networks.

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

## 3.0 Policy

General

1. It is the responsibility of employees with VPN privileges to secure the device and password so that unauthorized users are not allowed unintentional access to EMU internal networks.
2. All computers communicating to or from EMU networks via VPN or any other technology must have adequate anti-virus protection.
3. By using VPN technology with personal equipment, users must understand that their computing devices 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 (Section 8 -Division of Information Technology [DoIT] policies). Devices connected over a VPN to or from EMU are also considered part of the non-public network.

VPN connections from campus

1. VPN Connections made from EMU networks to external networks will be required to maintain compliance with the Division of Information Technology policies, standards and guidelines.
2. Any VPN connection may be disconnected by the Division of Information Technology for any reason, for any length of time including permanently.

VPN connections to campus

1. Access to the EMU VPN will be granted only to those individuals who possess a valid business case, upon their request, for up to one calendar year and must be requested again if a valid business need still exists to avoid an interruption of access.
2. 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.

## 4.0 Responsibility for Implementation

The Chief Information Officer and Director of Network and Systems are responsible for the implementation of this policy.

## 5.0 Enforcement

Any employee found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any student found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of state or federal laws will be reported to the appropriate legal authority for investigation.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

## 6.0 Definitions

| Term | Definition |
|---|---|
| VPN | Virtual Private Network: an encrypted, private network connection. |
| | |
| | |

## 7.0 Revision History

| Description | Approval Date |
|---|---|
| Revised based on new technology purchase | August 10, 2011 |
| Revised based on newer template | August 15, 2011 |
| Policy Committee | January 23, 2014 |
| Approved by CIO | January 27, 2014 |