

	Information and Communications Technology Division	Policy	
		Effective Date	Date of Last Revision
		May 3, 2006	May 3, 2006

Chapter Name	
6.0 NETWORKING	
Chapter Number	Title
6.1	Secure Networked Devices

1.0 Purpose

The purpose of this policy is to define the restrictions placed on all devices connected to the campus network, and the administrative privileges afforded to Eastern Michigan University (EMU) over these devices.

2.0 Scope

This policy covers all devices, University-owned or otherwise, connected to the campus data network.

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

This policy covers all connected devices. No previously existing connections will be grandfathered.

3.0 Policy

Information and Communications Technology (ICT) is assigned administrative responsibility for managing and securing the enterprise data network by the University. Within this responsibility, it is the policy of ICT to maintain a secure data network, ensuring both that communication across it and the devices connected to it are as protected as possible.

To this end, all devices connected to the non-public campus data network (wired or wireless, including VPN connections) are considered under the administrative control of authorized ICT staff, which includes the right to modify anything on the device that might need to be changed to maintain security, including but not limited to passwords, local accounts and software patches. All devices connected to the campus data network - including the public network – can be disconnected, scanned for security flaws, and prevented from connecting in the future by authorized ICT staff in order to protect the campus data networks and information contained therein.

Devices will not be permitted on the campus data network unless they meet current ICT security standards. These standards may change at any time at the discretion of authorized ICT staff.

1. As in all duties of their station, authorized ICT staff will be held accountable for their actions. Security scanning that is unnecessarily intrusive, irresponsible or malicious will not be tolerated under any circumstances.
2. A list of ICT staff authorized to modify security standards should be published where EMU employees can access it.
3. A list of ICT staff authorized to modify any networked devices should be published where EMU employees can access it.
4. Some security requirements necessary for a network connection may be non-public due to sensitive information, but these must be internally maintained by the ICT staff authorized to change them.

4.0 Responsibility for Implementation

The Director of IT Security Administration and the Director, IT Network and Systems are responsible for implementing this policy.

5.0 Enforcement

Enforcement will be handled by the Director of IT Security Administration and the 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>
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 Team	Initial Draft	May 17, 2005	
Barr	Revised	June 20, 2005	
French	Revised after Open Forum	July 12, 2005	
Popp	Submitted to CIO	July 28, 2005	May 3, 2006
Laundra	Copyedited & proofed for upload	May 3, 2006	