

Chapter Name

6.0 NETWORKING

Chapter Number Title

6.4 Secure Network Equipment Policy

1.0 Purpose

The purpose of this policy is to define the restrictions placed on all devices offering core services on or comprising the infrastructure of the campus network, and the control afforded to Division of Information Technology (DoIT) Network Engineering over these devices. While all devices connected to the network are covered by the [Secure Network Devices Policy \(6.1\)](#), additional restrictions contained in this policy cover network equipment.

2.0 Scope

This policy covers all core service and infrastructure devices -University-owned or otherwise - connected in any way to the campus data network, as defined by DoIT Network Engineering. Infrastructure devices include but are not limited to hubs, switches, bridges, routers, firewalls, intrusion detection system, and any other systems transporting or controlling data over the network. Core service devices include but are not limited to authentication systems, IP services such as DHCP and DNS, proxy servers, and any other service supporting or controlling data flow on the network. These will be referred to hereafter as network equipment.

Standard restrictions apply to all devices on the network as stated by the [Secured Network Devices Policy \(6.1\)](#). Further restrictions are imposed on network equipment as stated in the [Wireless Communication Policy \(6.2\)](#).

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

DoIT Network Engineering is assigned administrative responsibility for managing and securing the enterprise data network by the University. It is the duty of DoIT to maintain a secure data network, ensuring both that communication across it and the devices connected to it are as protected as possible.

Network equipment will not be permitted a connection to the campus data network – physical or virtual - unless it meets the requirements outlined in this policy.

1. Network equipment installation must be requested through and coordinated by DoIT Network Engineering via the Director IT, Network and Systems or Assistant Director IT, Network and Systems.
2. DoIT Network Engineering must approve of network equipment prior to connection.
3. DoIT Network Engineering will audit the configuration of any network equipment, and reserves the right to require changes prior to permitting connection.
4. The DoIT Security Office may audit the configuration of network equipment.
5. DoIT Network Engineering must retain complete administrative access over any connected network equipment.
6. Any control or reporting access to network equipment shall be restricted to DoIT Network Engineering unless specified in writing by both the Director of IT Security Administration and Director IT, Network and Systems.

7. Changes to network equipment must be approved by DoIT Network Engineering.
8. DoIT Network Engineering reserves the right to perform security audits on all network equipment configurations.
9. In accordance with Eastern Michigan University policy, DoIT Network Engineering reserves the right to monitor any data traversing network equipment, in the interests of security, performance, or fulfillment of a legal request.
10. DoIT Network Engineering may disconnect network equipment at any time in the interests of security or performance.

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 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 suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including discharge.
- Criminal prosecution.

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.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including suspension or expulsion from school.
- Criminal prosecution.

If you break the law, you can be prosecuted. Even if you are not charged criminally, you can be held personally liable, and you can be suspended or dismissed from the University, or fired if you are an employee.

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

| <u>Term</u> | <u>Definition</u> |
|----------------|---|
| Devices | Anything connected to an Eastern Michigan University network in any way, whether physically cabled, wireless, indirectly via virtual connections, or otherwise. |

| | |
|---------------------|---|
| DHCP | Dynamic Host Configuration Protocol, a protocol that allows devices to request IP addresses and other configuration settings from a server |
| DNS | Domain Name System, a system that associates information with domain names. Examples including associating IP addresses with hostnames, and mail server addresses with domain names. |
| Equipment | Any networked device that can be further classified as an infrastructure device, which is any device monitoring, supplying or facilitating core services or access to the network. Examples of infrastructure devices include but are not limited to hubs ,switches, bridges, routers, firewalls, sniffers, intrusion detection system, and any other systems transporting or controlling data over the network. Core service devices include but are not limited to authentication systems, IP services such as DHCP and DNS, proxy servers, and any other service monitoring, supporting or controlling data flow on the network Rom. |
| Proxy server | A computer or other device that allows network clients to indirectly make use of other network services |

| 7.0 Revision History | | | |
|--------------------------------|--|------------------------|----------------------|
| <u>Creator</u> | <u>Description</u> | <u>Submission Date</u> | <u>Approval Date</u> |
| DOIT Security | DOIT Security Team | March 10, 2006 | |
| DOIT Security | Reviewed | December 12, 2006 | |
| French | Revised | December 13, 2006 | |
| CP | Edits per PRC team meeting | June 15, 2007 | |
| A. Barr | Housekeeping edits to conform with change to IT; misc. minor typographical edits- | January 12, 2009 | |
| A. Barr | Note this previously held number 6.3 but was changed to resolve conflict with 6.3 Open Area Network Security | January 12, 2009 | |
| DoIT Policy Committee | Reviewed policy and suggested modifications to clarify language; add authority to audit configuration of network devices to DoIT Security Office | January 13, 2009 | |
| A. Barr | Make changes suggested by Policy Committee | January 13, 2009 | |
| A. Barr | Delete “also” from Section 3. Paragraph 4. -- Final Spell Check. | January 14, 2009 | |
| Town Hall and Policy Committee | Reviewed and discussed; explanation for consequences language added to Section 5 and removal of prior statement on penalties. Revised version posted to Policy Web site under Proposed Polices | January 27, 2009 | |
| A. Barr | Submitted to CIO for Review and Approval. | January 27, 2009 | October 2, 2009 |
| A. Barr | Finalized for Web and uploaded to Website. | October 2, 2009 | |