EMPORIA STATE UNIVERSITY™

			10.6.1
Division:	Technology & Computing Services	Effective Date:	10/20/2006
Department	Information Security	Last Revised:	10/03/2006
Version:	FSB 06011	Next Annual Review:	01/31/2007
Approved By:	Faculty Senate and University President	Date Passed Senate:	10/03/2006
		Date of ESU President's Approval:	10/20/2006
Previous Action:			

Network Controls (FSB 06011 approved by President 10/20/06)

Policy Objectives

Emporia State University (ESU) is committed to maintaining the confidentiality, integrity, and accessibility of the information it owns or controls.

Access to these assets is provided by several avenues. These include: wired network, wireless network, dial-in, and VPN. The avenues that ESU provides for access are protected by policies, standards, guidelines and other security measures including, but not limited to, firewalls and intrusion detection devices.

As our external defenses get stronger, crackers look for easier ways to infiltrate our network. One example of accomplishing this is called War dialing; where crackers dial every number associated with an organization looking for a modem to answer. Once they find a modem on our network that may have weak controls, they have access to other areas of our network putting university information at risk.

This policy sets out to ensure that all avenues into our network are approved and properly secured.

Policy

Network access devices not approved and managed by Technology & Computing Services (TCS) are forbidden. Examples of such devices include but not limited to:

- Modems
- Wireless access points
- Network switches and hubs

Responsibilities

All users are responsible for taking the steps necessary to protect university information. This includes:

- Using only approved and authorized means to connect to ESU's network
- Obtaining proper approval before connecting any access device to ESU's network
- Notifying the Information Security Officer (ISO) of any variance to this policy

TCS is responsible for monitoring compliance with this policy.

Scope

This policy applies to all network access devices connected to the ESU network.

Enforcement

The ISO is responsible for monitoring and reporting compliance with this policy.

In all cases, information will be disclosed as required by controlling law.

Exceptions

The President or designee must approve any exceptions to this policy.

			10.6.1
Division:	Technology & Computing Services	Effective Date:	10/20/2006
Department	Information Security	Last Revised:	10/03/2006
Version:	FSB 06011	Next Annual Review:	01/31/2007
Approved By:	Faculty Senate and University President	Date Passed Senate:	10/03/2006
		Date of ESU President's Approval:	10/20/2006
Previous Action:			