EMPORIA STATE UNIVERSITY

| | | | |
|---|---|---|---|
| | | | 10.4.1 |
| Division: | Technology & Computing Services | Effective Date: | 10/20/2006 |
| Department | Information Security | Last Revised: | 04/10/2009 |
| Version: | FSB 06002 | 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: | | | |

# Controls Against Malicious Software (FSB 06002 approved by President 10/20/06)

## Policy Objectives

Emporia State University (ESU) is committed to maintaining the confidentiality, integrity, and accessibility of the information assets it owns or controls.  One threat to ESU's information assets is malware, otherwise known as viruses, trojans, worms, and spyware.  Should a self-propagating worm like CodeRed gain access to our network all legitimate network traffic would be brought to a standstill.  While worms like CodeRed take up bandwidth making normal network communications difficult, other malware may destroy critical data or make it easy for unauthorized access to our resources.  The risks to ESU's information can be greatly reduced if all workstations have active anti-virus software and the software is kept up to date.

This policy sets out to ensure that computing devices within the ESU network environment are protected from malware to the best of our ability.

## Policy

All workstations connecting to the ESU network environment must have approved anti-virus software installed and running.  Virus definitions for that software must be updated weekly or as directed by Technology & Computing Services (TCS) staff.

Procedures for obtaining approved software and for updating anti-virus definitions can be found in the Controls Against Malicious Software Standards.

## Responsibilities

It is the responsibility of each user to ensure that the workstation they are using has an approved copy of anti-virus software installed and running with automatic updates enabled.

It is the responsibility of TCS staff to provide a licensed copy of approved anti-virus software to each ESU owned and maintained workstation and to periodically audit for compliance with this policy.

Students who do not own approved anti-virus software must obtain a licensed copy.

## Scope

This policy applies to all wired and wireless workstations connecting to the university network.

## Enforcement

Workstations found to be out of compliance with this policy may be blocked from the network until such time as they become compliant.

The Information Security Officer 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.