			7.1.3
Division:	Technology & Computing Services	Effective Date:	03/10/2010
Department	Information Security	Last Revised:	03/02/2010
Version:	FSB09010	Next Annual Review:	03/10/2011
Approved By:	Faculty Senate and University President	Date Passed Senate:	03/02/2010
		Date of ESU President's Approval:	03/10/2010
Previous Action:			

Information Technology Usage Policy

Policy Objectives

The purpose of this policy is to outline the acceptable uses of computing and information technology resources at Emporia State University ("University").

Policy

It is University policy to provide computing and information technology resources to faculty, staff, students, official University affiliates, and others in support of the education, research, and public service missions of the university.

Users of University computing and information technology resources are responsible for using these resources only as allowed by law and in connection with the University's core teaching, research, service, and other identified missions. Users must abide by the following standards of acceptable use:

- Users shall abide by all applicable state and federal laws, all University and Board of Regents policies, and all applicable contracts and licenses
- Each user is responsible for the activities that occur while they are using the computing and technology resources assigned to them and will use only those computing and information technology resources for which the individual has authorization and only in the manner and extent authorized
- Users shall respect the copyright and intellectual property rights of others and ensure the legal use of copyrighted material
- Users shall use computing and information technology resources in a manner that does not interfere with, compromise, or harm the University's computing and information technology resources

Uses of University computing and information technology that do not significantly consume resources or interfere with other users may also be acceptable, but may be restricted by Technology and Computing Services (TCS) upon advice of the University President, or his/her designee. Under no circumstances shall members of the University community or others use University information technology resources in ways that are illegal, that threaten the University's tax-exempt status, or that interfere with reasonable use by others members of the University community.

Access to University computing and information technology resources requires appropriate permission and access to resources is not guaranteed.

The extension of these privileges is predicated upon the user's acceptance of and adherence to the corresponding user responsibilities detailed in this policy and other applicable policies and laws. The University reserves the right to limit, restrict, or extend access to information technology resources without prior notice in order to protect university resources.

Confidentiality and Privacy

Communications made using University computing and information technology resources are considered to be non-confidential communications. There is no expectation of privacy regarding such communications, which may be subject to access and disclosure under the Kansas Open Records Act (KORA). Confidential information should not be sent using email unless encrypted using a University supplied encryption product. Examples of such confidential information include but are not limited to records and data subject to the Family Educational Rights and Privacy Act (FERPA) and implementing regulations.

In general, information stored on university owned equipment and resources will be treated as confidential. However, the user of such equipment should have no expectation of personal privacy or confidentiality of documents and messages stored on University owned equipment and resources. Additionally, information stored on University networks may be accessed by the University for purposes related to security management, system operations, and legal compliance.

Reporting violations

Users and departments will report any discovered unauthorized access attempts or other improper usage of University computing and technology resources to the Chief Information Officer (CIO), the Information Security Officer (ISO), or other appropriate administrator as per the Information Security Incident Reporting Procedures.

Consequences for violations

Persons in violation of this policy are subject to the full range of sanctions, including but not limited to, the suspension of system privileges.

At the time, if disciplinary procedures are initiated, in accordance with published policies and rules of conduct, the person alleged to be in violation of the policy will be notified of the alleged violation.

Suspension of system privileges for students may also be handled according to the procedures outlined in the Student Code of Conduct.

Division:	Technology & Computing Services	Effective Date:	03/10/2010
Department	Information Security	Last Revised:	03/02/2010
Version:	FSB09010	Next Annual Review:	03/10/2011
Approved By:	Faculty Senate and University President	Date Passed Senate:	03/02/2010
		Date of ESU President's Approval:	03/10/2010
Previous Action:			

Responsibility

The CIO will be responsible for:

- Determining and posting operational policies, networking standards and procedures in consultation with university governing bodies so as to implement the principles outlined in this policy
- Reviewing and updating this policy in consultation with the relevant University governance structure

TCS has the responsibility to protect shared information technology services. In the event of hardware or software failure, or in the event of an attack by malicious user(s), designated TCS staff will quarantine any technology resources necessary to solve the problem, to protect the system, and the information the system contains.

The Information Security Officer is responsible for working with TCS and Unit Support personnel to implement a network logon banner using the Logon Banner Standards.

Authorized users of University computing and information technology resources are responsible for reviewing and following published Information Security policies and procedures.

Scope

This policy applies to faculty, staff, students, official university affiliates, and any other individual who uses University computing and information technology resources.

Enforcement

The CIO 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.