

Date Passed Senate: October 6, 2009

Date of ESU President's Approval: October 13, 2009

FSB 09006

ENCRYPTION POLICY

Date of First Reading: September 15, 2009

Date of Second Reading: October 6, 2009

Senate Sponsor: Academic Affairs Committee
Ann O'Neill, Chair of Academic Affairs

- I. **Purpose:** To create a policy regarding encryption when protected information is transmitted via email, FTP or other means.

- II. **Previous Senate Action:** None

- III. **Rationale (optional):** In 2008 Emporia State University was audited by the Legislative Division of Post Audit. After consultation with the University General Counsel, the Academic Affairs committee and the University Information Security Officer, Cheryl O'Dell, CISSP (Certified Information System Security Professional) have drafted an encryption policy to reflect the expectations of the audit findings.

- IV. **Guidance (optional):** When information protected by privacy laws or rights is transmitted either via email or FTP or through an attachment to an email, it is possible for entities to do "packet sniffing" (e.g., eavesdropping) and see the information when no encryption is used. There are various ways to use encryption when needing to transmit protected information; through SSL using https, special encryption software, using a Virtual Private Network connection as well as other ways to encrypt e-mail and attachments.

FSB 09006

Encryption Policy

- 1
- 2 Policy Objectives
- 3
- 4 Emporia State University (ESU) maintains information for business and academic use
- 5 which at times might need to be transmitted. When transmitting sensitive data, data
- 6 encryption techniques should be used to control access to the information, protect the
- 7 integrity of transactions, and protect ESU's information assets.

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46

Policy

ESU users transmitting information protected by privacy laws and rights will use encryption when transmitting to off campus entities.

Responsibility

Technology & Computing Services (TCS) will be responsible for identifying appropriate encryption methodologies for transmission of information protected by privacy laws and rights. Encryption methodologies include, but are not limited to:

- Virtual Private Network (VPN)
- Secure Socket Layer (SSL)
- Public Key Infrastructure (PKI) (e.g., digital id's for secure email)
- Encryption Software

Units may be responsible for the licensing cost of third party solutions as necessary.

Users transmitting information protected by privacy laws and rights are responsible for contacting the Information Security Officer (ISO) regarding the type of encryption which should be used.

The ISO will be responsible to raise awareness about when encryption should be used to help educate the ESU community.

Scope

This policy applies to all persons granted access to ESU's information systems when transmitting protected information to off campus entities.

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.

Provide comments about this bill to your department's senator or Faculty President Carol Russell at crussell@emporia.edu.