

Date Passed Senate: October 6, 2009

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

FSB 09002

INFORMATION TECHNOLOGY RISK ASSESSMENT 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 risk assessment of information technology systems for information security purposes.

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 information technology risk assessment policy to reflect the expectations of the audit findings.

IV. Guidance (optional): Audits of ESU systems need to be done periodically to reveal any new risks. When new technology is introduced into the ESU network, risk assessments are done to verify information security policies, procedures and standards are used.

FSB 09002

Information Technology Risk Assessment Policy

- 1
- 2 Policy Objectives
- 3
- 4 Information Technology (IT) security assurance is the degree of confidence with which
- 5 managerial, technical, and operational security controls protect the information assets of
- 6 Emporia State University (ESU). Administrators must understand the current status of
- 7 the systems' security controls in order to make informed decisions and investments that
- 8 appropriately mitigate Information Security risks to an acceptable level.
- 9
- 10 Policy

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
47
48
49

ESU will conduct formal Risk Assessments of enterprise wide IT systems, information management processes, and information practices annually and as needed using methods identified in the Risk Assessment Procedures. The risk assessment findings, the controls identified, and a risk rating will be developed into the Information Security Assessment report for review by the Chief Information Officer (CIO) and the system administrator to determine risk mitigation and information security measures.

Responsibility

The Information Security Officer has the responsibility to:

- Develop and maintain formal Risk Assessment Procedures
- Work with Technology and Computing Services (TCS) and Unit Support personnel to identify risks of the institution’s information systems and infrastructure and the controls required to mitigate identified risks
- Work with the CIO to determine the risk ratings
- Develop the Information Security Assessment report

When investments in controls are warranted:

- TCS will be responsible for implementing the controls on systems managed by TCS
- Unit Support Personnel will be responsible for implementing the controls on systems they manage

Scope

This policy applies to all technology related infrastructure devices including but not limited to: servers, workstations, routing and switching devices, and telephone systems owned or maintained by ESU.

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.

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