

Date Passed Senate: October 6, 2009

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

FSB 09003

CHANGE CONTROL 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 change control for enterprise 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 a change control policy to reflect the expectations of the audit findings.
- IV. **Guidance (optional):**Controlling when updates are applied to university wide systems or desktop operating systems is necessary so proper testing can be performed to 1) identify any issues which may make the system(s) unusable; 2) identify any changes or features so faculty and other users can be made aware; 3) test the upgrade process; 4) verify the system will be usable by the ESU owned computers. If new technologies are put into place without proper testing, the new technology may not work at ESU. This policy is to help keep availability of systems used campus wide optimal. There may be systems managed by unit support personnel, which if changed might impact a large group of faculty and student users. The unit support personnel managing those types of systems are encouraged to follow the same type of procedures before introducing a change.

FSB 09003

Change Control Policy

- 1
- 2 Policy Objectives
- 3

4 Emporia State University (ESU) understands inappropriate introduction of upgraded
5 software can impact the integrity and confidentiality of computing systems, the services
6 they provide, and the data that resides within them. In addition, an improperly prepared
7 or implemented change to infrastructure or systems can significantly impact availability
8 of key systems. A change is defined as but not limited to:

- 9 • Upgrade to software or hardware of an enterprise system or server
- 10 • Enhancement or deployment of new server or server functionality
- 11 • Upgrade of network infrastructure or telephone system

12 This policy outlines ESU's commitment to adopt standard methods and procedures when
13 altering the Information Technology environment in order to minimize the risk of
14 negative impacts to information and technology services offered and managed by
15 Technology and Computing Services (TCS).

16 Policy

17
18
19 Formal Change Control Procedures must be followed for installation and modification of
20 any Information Technology infrastructure or enterprise system managed by TCS,
21 including but not limited to servers, software, telecommunications, and network
22 infrastructure.

23 Responsibility

24
25
26 Unit Support Personnel are encouraged to follow the Change Control Procedures
27 developed by TCS on systems they manage.

28
29 The Information Security Officer (ISO) has the responsibility to:

- 30 • Work with TCS teams to develop, support, and maintain formal Change
31 Control Procedures for university systems and infrastructure managed by TCS
- 32 • Advise Unit Support Personnel to consider adopting formal Change Control
33 Procedures

34
35 TCS personnel have the responsibility to:

- 36 • Identify the need for changes and originate a Request For Change (RFC) as
37 per the Change Control Procedures and provide input for the TCS
38 management team and stakeholder groups as needed for review of request
- 39 • Review, test, communicate and implement approved changes to affected
40 stakeholders

41 Scope

42
43
44 This policy applies to all Information Technology services, servers, and infrastructure
45 managed by TCS and Unit Support Personnel.

46 Enforcement

47
48

49 The CIO or designee is responsible for monitoring and reporting compliance with this
50 policy.

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

52

53 Exceptions

54

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

56

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