

Date Passed Senate: 18 November 2008

Date of ESU President's Approval: 18 November 2008

## **FSB 08004**

### **CLEAR DESK AND CLEAR SCREEN POLICY**

Date of First Reading: 4 November 2008

Date of Second Reading: 18 November 2008

Senate Sponsor: Academic Affairs Committee  
Dwight Moore, Chair of Academic Affairs

**I. Purpose:** To establish a Faculty Senate approved policy that will provide guidance in the protection of private information.

**II. Previous Senate Action:** none

**III. Rationale:** In 2004 Emporia State University, together with Kansas State University and the University of Kansas, was audited by the Legislative Division of Post Audit to determine its information security status. In April 2005 the University received the results of that information security audit in the form of two reports: One confidential report, for obvious reasons, had very limited distribution, and one public. A number of findings from that audit recommended the adoption of substantial policies written and adopted to secure the information assets and infrastructure of the University.

In collaboration with a professional security consultant, our Information Security Officer, Cheryl O'Dell, CISSP (Certified Information System Security Professional), drafted twenty policies to reflect the expectations of the audit findings. The Administrative Team adopted these twenty policies as "Interim" on January 31, 2006. However, the policy on Clear Desk and Clear Screen was not approved by the faculty senate in 2006 when 18 of the 20 policies were approved.

**IV. Guidance:** This policy will provide substantial improvements in system and information security.

---

## **FSB 08004**

### **Clear Desk and Clear Screen Policy**

#### **Policy Objectives**

Emporia State University (ESU) is committed to maintaining the confidentiality, integrity, and accessibility of the information assets it owns or controls. To assist in

this effort, policies, standards, and guidelines will be developed and promulgated throughout the ESU community.

These information assets can be in many forms. They can range from a piece of paper or a Post-It® note to digital forms such as data stored on a hard-drive or university information accessible from computer workstations.

When a work area is left unattended, anyone passing by could have access to all information left on or around the desk as well as all electronic information that a user has access to if that user remained logged onto the workstation.

This policy sets out to ensure that all forms of information used in and around a work area is protected from unauthorized viewing or altering while the area is unattended.

#### Policy

University information protected by privacy laws and rights should not be left visible to visitors in a work area, whether the information is in electronic or paper form.

#### Responsibilities

All users are expected to protect the information for which they are responsible. This includes:

- Configuring a screensaver password as per Screensaver Standards
- Paperwork containing information protected by privacy laws and rights will not be left in full view of unauthorized personnel

#### Scope

This policy applies to all persons entrusted with access to information protected by privacy laws and rights.

#### Enforcement

Supervisors are responsible for ensuring that their employees follow this policy. TCS is responsible for monitoring ESU workstations for 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.