Physical and Environmental Security Policy
Kansas State University
January 21, 2009

Table of Contents

.010 Purpose

This policy defines the requirements for protecting university information and technology resources from physical and environmental threats in order to prevent loss, theft, damage, or unauthorized access to those resources, or interference with K-State operations.

.020 Scope

This policy applies to all university colleges, departments, administrative units, and affiliated organizations that use university information technology resources to create, access, store or manage University Data to perform their business functions.

.030 Effective Date

This policy will be effective upon approval by the Computing Executive Committee [*replace with date after CEC approval*].

.050 Policy

All University information and technology resources should have appropriate physical and environmental security controls applied commensurate with identified risks.

.060 Definitions

A. *Mobile Storage Devices*- Any easily movable device that stores University Data, including but not limited to laptop computers, PDA's, and USB flash drives.

B. *Uninterruptable Power Supply (UPS)* – A device designed to provide power, without delay, during any period when the normal power supply is incapable of performing acceptably.

C. *University Data* – Any data related to Kansas State University ("University") functions that are a) stored on University information technology systems, b) maintained by K-State faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

.070 Roles and Responsibilities

Responsibility for physical and environmental security of K-State information and technology resources is shared by the individuals using these systems, units that own them, and system administrators responsible for managing the systems.

.080 Implementing Procedures

A. *Network wiring and equipment* – Network wiring and equipment closets and cabinets must be locked when unattended. Other network cabling and devices should likewise be physically secured where feasible. Access to core and building distribution network facilities must be limited to authorized network support personnel and all visitors escorted by said personnel. Date and time of entry and departure for core network facilities should be recorded.

B. *Office doors* – All office doors should remain locked after hours or when offices are unattended for a prolonged period of time.

C. *Mobile storage devices* – Mobile storage devices, such as laptop computers or USB drives, should be stored securely when unattended. Appropriate secure storage methods include a locking security cable attached directly to the device, storage in a locked cabinet or closet, storage in a locked private office, or the like. Encrypting data stored on mobile devices, such as whole disk encryption on laptop computers, likewise reduces the risk of a breach of University Data resulting from theft, loss, or unauthorized access. When traveling with mobile storage devices or using them in public places, appropriate security precautions should be taken to prevent loss, theft, damage, or unauthorized access. Use of tracking and recovery software on laptop computers is encouraged.

D. *Electrical power* – Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable power supplies (UPS) with sufficient capacity to provide at least 30 minutes of uptime to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Systems hosting confidential data should also be protected with a standby power generator where feasible.

.090 Related Laws, Regulations, or Policies

A. Kansas State University Data Classification and Security Policy

B. K-State Network/Telecommunications Space Accommodations Policy specifies physical security for network and telecommunications facilities (www.k-state.edu/its/itpolicies/accomodation.pdf)

C. State of Kansas Information Technology Policy 7230 – *General Information Technology Enterprise Security Policy* (www.da.ks.gov/itec/Documents/itecitpolicy7230.htm)

D. State of Kansas *Default Information Technology Security Requirements* (www.da.ks.gov/itec/Documents/ITECITPolicy7230A.pdf), March 2006

E. ISO/IEC 27002:2005, "Information technology – Security techniques – Code of practice for information security management" (www.iso.org/iso/catalogue_detail?csnumber=50297), published by the International Standards Organization (www.iso.org). This is an international security standard that specifies physical and environmental security controls to protect assets from loss, theft, damage, and unauthorized access.

.100 Questions/Waivers

The Vice Provost for Information Technology Services is responsible for this policy. Questions relating to this policy should be directed to the Chief Information Security Officer.