System Development and Maintenance Security Policy
Kansas State University
April 14, 2009, *revised April 29, 2009*

Table of Contents

.010 Purpose

The purpose of this policy is to define requirements for system security planning and management to improve protection of University information system resources. Security has to be considered at all stages of the life cycle of an information system (i.e., feasibility, planning, development, implementation, maintenance, and retirement) in order to: a) ensure conformance with all appropriate security requirements, b) protect sensitive information throughout its life cycle, c) facilitate efficient implementation of security controls, d) prevent the introduction of new risks when the system is modified, and e) ensure proper removal of data when the system is retired. This policy provides guidance to ensure that systems security is considered during the development and maintenance stages of an information system's life cycle.

.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. The requirements apply to enterprise information systems or systems that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein.

.030 Effective Date

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

.050 Policy

Appropriate security controls should be considered at all stages of an information system life cycle, including the development and maintenance stages.

A. *System security plans and documentation* – System security plans and documentation must be prepared for all enterprise information systems or other systems under development that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein. Such plans should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements through all stages of the system's life cycle. When the system is modified in a manner that affects security, system documentation must be ~~reviewed and~~ updated accordingly.

B. *Separate development, testing, and production environments* – System development, testing, and production should be performed in separate environments.

C. *Test data* – Testing of enterprise information systems should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with ~~the~~ any confidential data appropriately sanitized. Testing should not ~~never~~ be done on live data due to the threat to its confidentiality and/or integrity. ~~risk of corruption and/or breach~~. Testing that requires the use of live data or confidential data must have appropriate security controls employed.

D. *Vulnerability management* – An assessment of the system's security controls and a vulnerability assessment that seeks to identify weaknesses that may be exploited must be performed on all new enterprise information systems or ones undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production enterprise information systems and appropriate measures taken to address the risk associated with identified vulnerabilities. Vulnerability notifications from vendors and other appropriate sources should be monitored and assessed for all systems and applications associated with enterprise information system.

E. *Vendor acquisitions* – If an enterprise information system or component of that system is acquired from an external vendor, ~~the vendor must provide~~ written documentation must be provided that specifies how the ~~specifying how their~~ product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow testing of the system's security controls by K-State or an independent third party, if needed.

.060 Definitions

A. *Confidential data* – Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. See K-State's *Data Classification and Security Policy* for an expanded definition and examples.

B. *Enterprise information system* – An information system and/or server providing services commonly needed by the University community and typically provided by central IT units. Departmental information systems provide services specific to the mission and focus of individual Colleges, departments, administrative units, or affiliated organizations and are typically provided by distributed IT staff in those units.

C. *Live data* – data accessible to users through systems that are in production (i.e., *live*).

D. *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

A. *Chief Information Security Officer (CISO)* – Coordinates the development of guidance for the development, review, and approval of system security plans as well as the identification, implementation, and assessment of common security controls; oversees periodic vulnerability assessments for enterprise information systems; and coordinates implementation of other assessments as needed with information system security administrators.

B. *Information System Security Administrator* – Ensures the application of appropriate operational security controls for an information system; coordinates with the CISO in the identification, implementation, and assessment of common security controls; plays an active role in developing and updating a system security plan and coordinating with an information system owner any changes to the system and assessing the security impact of those changes. This role may be filled by someone directly involved with the development, maintenance, and/or operation of the information system.

.090 Related Laws, Regulations, or Policies

A. *Existing K-State systems development and maintenance policies*

1. *Security patches* –K-State's requirements for keeping systems and applications is in K-State's "Security for Computing, and Network Resources" policy in PPM 3430, section .050, "Security Patches" (www.k-state.edu/policies/ppm/3430.html#require).

B. *Other related laws, regulations, or policies*

1. Kansas State University *Data Classification and Security Policy* [will insert the URL when the policy is published].

2. Kansas State University *Media Sanitization and Disposal Policy* [Draft]

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

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

5. 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 security requirements for controlling access (see chapter 11, "Access control") to ensure access to information and information systems is limited to authorized users.

6. NIST Special Publication 800-18, revision 1; *Guide for Developing Security Plans for Federal Information Systems,* National Institute of Standards and Technology, February 2006.

.100 Questions/Waivers

The Vice Provost for Information Technology Services (VP ITS) is responsible for this policy. The VP ITS or designee must approve any exception to this policy. Questions relating to this policy should be directed to the Chief Information Security Officer.