Operations and Management Security Policy
Kansas State University

May 13, 2009, *Revised August 7, 2009*

Table of Contents

.010 Purpose

The purpose of this policy is to help ensure the secure operation of K-State information systems and proper management of K-State's IT security program and technologies.

.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*].

.040 Authority

The state of Kansas Information Technology Executive Council (ITEC) policy 5300 Revision 1, *Business Contingency Planning,* requires all state agencies, including Regents institutions, to develop "business continuity plans to ensure that all entities can continue critical operations during any disruption and resume normal operations within a reasonable period of time."

ITEC policy 7310, *Information Technology Security Self-Assessment Policy*, requires all state agencies, including Regents institutions, to complete an annual self-assessment of the status of the security of its information systems.

.050 Policy

A. *Business continuity plan* – Kansas State University must have a business continuity plan to guide recovery from disasters or other major disruptions to service in a manner that maintains the security of K-State information systems and ensures timely restoration of services.

B. *Configuration management* – the configuration of servers, workstations, network devices, firewalls and other enterprise security technologies should be managed in a way that provides consistent setup, documents changes, and ensures security requirements are maintained when the configuration is changed.

C. *Data backups* – University Data must be backed up regularly and backup media stored securely.

D. *Firewalls*

1. All connections to networks outside the K-State campus, such as the Internet and Internet2, must be protected with a firewall that filters both incoming and outgoing network traffic against common threats.
2. All enterprise information systems and any K-State system hosting confidential data must be protected by a network firewall and a host-based software firewall, both configured in "default deny" mode for incoming traffic and enforcing documented trust relationships for those systems.
3. All K-State computers must have a host-based firewall configured appropriately for the security requirements of the system and the classification of data stored therein.
4. Logging should be enabled for all firewalls and periodically reviewed for anomalous events.
5. Configuration of network firewalls and host-based firewalls on enterprise information systems should be audited periodically to ensure consistency with the security requirements of the system(s) they protect.

E. *Security event logging and auditing*

1. Audit logs recording user activities, exceptions (i.e., errors or failures), and information security events should be generated commensurate with the security requirements of the system being monitored. Audit logs should be retained for at least 30 days.
2. Enterprise information systems must log system administrator activities, such as the use of privileged accounts (e.g., supervisor, administrator, or root).
3. Audit logs should be periodically reviewed to detect security violations.
4. Security event log data must be protected against unauthorized access and alteration.
5. Clocks of systems being monitored should be synchronized regularly from an accurate time source.

F. *Security management* – K-State's IT security program and policies must be monitored and periodically assessed to ensure their continued effectiveness. The Chief Information

Security Officer or designee must perform an annual IT security self-assessment and submit a summary report to the Kansas Board of Regents office, as required by state of Kansas information technology policy.

.060 Definitions

A. *Authentication* – Process of verifying one's digital identity. For example, when someone logs into Webmail, the password verifies that the person logging in is the owner of the eID. The verification process is called authentication.

B. *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.

C. *Default Deny* – a firewall ruleset that begins with blocking *all* network traffic, both incoming and outgoing, then only allowing specific network traffic required for the effective and secure operation of the system(s) protected by the firewall.

D. *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.

E. *Firewall* - A specialized device or software program that controls the flow of network traffic between networks or hosts to enforce security policies and provide protection for the resources on those networks or hosts. For the purposes of this policy, a router with Access Control Lists (ACLs) is not considered a firewall.

F. *Trust relationships* – A specification of the level of access granted to computer systems and/or applications that are trusted to access resources on a server and its associated data and applications. This applies to access controls between systems, not access rights for individual users or roles.

G. *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 guidelines, standards, and/or procedures related to this policy as well as the identification, implementation, and assessment of common security controls needed for this policy; monitors and periodically assesses K-State's overall IT security program and policies; and ensures completion of an annual IT security self-assessment and report.

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; ensures that backups are being performed regularly and stored securely; and ensures that components of an information system have an appropriate system of configuration management in place.

.080 Implementing Procedures

A. *Security event logging and auditing*

1. Audit logs should include the following information, when relevant:
   a. eID or username
   b. Date and time of event
   c. Type of event
   d. Description of the event
   e. Network addresses and protocols involved
   f. Files accessed
   g. Commands/processes executed
2. K-State information systems should consider logging the following events and any others deemed appropriate for tracking important or suspicious actions:
   a. Successful and unsuccessful login or authentication attempts
   b. Access to confidential data
   c. Changes to access privileges for confidential data
   d. Activation and de-activation of security systems such as firewalls, anti-virus systems, and intrusion detection systems, and alerts from these systems
   e. Privileged operations such as the use of privileged accounts (e.g., supervisor, administrator, or root), system start-up and stop, and I/O device attachment/detachment
   f. System and network alerts and failure messages
   g. Changes to, or attempts to change, system security settings and controls

.090 Related Laws, Regulations, or Policies

A. *Existing K-State IT security operations and management policies*

1. *Vulnerability management* –K-State's requirements for assessing a system's security controls and identifying and mitigating vulnerabilities is in K-State's "System Development and Maintenance Security Policy" section .050.D (currently in draft undergoing review).

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. State of Kansas Information Technology policy 5300 Revision 1 - *Business Contingency Planning* (http://www.da.ks.gov/itec/Documents/ITECITPolicy5300.htm)

3. State of Kansas Information Technology Policy 7310, *Information Technology Security Self-Assessment Policy* (http://www.da.ks.gov/itec/Documents/ITECITPolicy7310.htm)

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

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

6. 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 10, "Communications and operations management") to ensure "the correct and secure operation of information processing facilities."

7. NIST Special Publication 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* (http://csrc.nist.gov/publications/drafts/800-41-Rev1/Draft-SP800-41rev1.pdf), July 2008

.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.