Access Controls Security Policy
Kansas State University

February 18, 2009, *revised July 28, 2009*

Table of Contents

.010 Purpose

Access controls are the rules that an organization applies in order to control access to its information assets. The risks of using inadequate access controls range from inconvenience to critical loss or corruption of data. This policy defines access control standards for system use notices, remote access, and definition and documentation of trust relationships for K-State information systems.

.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

Access control standards for K-State information systems are to be established in a manner that carefully balances restrictions that prevent unauthorized access to information and services against the need for unhindered access for authorized users.

A. *System use notice* – Before a user gains access to a K-State computer, a general system use notice must be displayed that welcomes users and identifies it as a K-State system, warns against unauthorized use of the computer, ~~provides notice of legal rights of the users,~~ and indicates that use of the system implies consent to all relevant K-State policies. The general system use notice should also be displayed before a user gains access to a K-State information system, where practical.

The system use notice must state the following:

> *Welcome to Kansas State University's information technology resources. Access to this system and all other electronic resources at K-State is restricted to employees, students, or individuals authorized by the University or its affiliates. Use of this system constitutes agreement to abide by all relevant K-State policies. Unauthorized or inappropriate use may result in limitation or revocation of use privileges and/or administrative, civil, or criminal penalties.*

B. *Remote access* – Remote access control procedures must provide appropriate safeguards through appropriate identification, authentication, and encryption techniques. *Direct* log-on to campus computers from off-campus locations is not allowed. A remote user must first authenticate to an authorized campus remote access service with strong encryption, such as K-State's VPN service or a departmental Windows Terminal Services (aka Remote Desktop Services) or Secure Shell (ssh) server, before logging into a campus computer. This restriction does *not* apply to authenticated user access to web applications like iSIS, K-State Online, Webmail, or to systems designed for public access.

For additional security controls for remote access, see "Data Security Standards," in K-State's *Data Classification and Security Policy*.

C. *Trust relationships* – Trust relationships for centrally-managed University information systems or any system with confidential data must be defined and documented, approved by an appropriate authority, and periodically reviewed and revised as needed. Security controls, such as firewall rulesets, must be configured to enforce the trust relationships. ~~The University Chief Information Security Officer (CISO) is responsible for developing guidance on documentation and approval of trust relationships.~~ *[moved to ".070 Roles and Responsibilities" section]*

.060 Definitions

A. *Authentication* – Process of verifying one's digital identity. For example, when someone logs into a workstation or server with their eID, 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. *K-State Computer* – Any computer considered to be the property of Kansas State University.

D. *Local Network* – Any segment of K-State's data network physically located on the Manhattan or Salina campus. This includes devices on the network assigned any routable and non-routable IP addresses, typically 129.130.X.X or 10.X.X.X, respectively, and applies to the wireless network and the network serving K-State's student residence halls and Jardine Apartments.

E. *Remote Access* - Accessing a K-State local network from any physical location outside the Manhattan or Salina campus. This includes access from off campus using K-State's VPN service.

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).

H. *VPN* – Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

.070 Roles and Responsibilities

A. *Chief Information Security Officer* – is responsible for developing guidance on documentation and approval of trust relationships.

.080 Implementing Procedures

A. The System Use Notice should be passively displayed such that no user action is required to view it before logging into the K-State computer or information system.

.090 Related Laws, Regulations, or Policies

A. *Additional K-State access control policies*

1. *Data access controls* – access controls based on data classifications are specified in K-State's *Data Classification and Security Policy*

2. *Password security* – Passwords are commonly used in conjunction with an identifying username to control access to information and information systems. K-State's password requirements are listed in K-State's "Security for Computing, and Network Resources" policy in PPM 3430, (www.k-state.edu/policies/ppm/3430.html#require).

3. *Unattended computers* – security controls for preventing unauthorized access to unattended computers are defined in K-State's "Security for Computing, and Network Resources" policy in PPM 3430, (www.k-state.edu/policies/ppm/3430.html#require).

4. *Vendor access* – access controls for vendors or other third parties who need to access K-State information systems for business reasons are defined in K-State's *Data Classification and Security Policy*

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

1. Kansas State University *Data Classification and Security Policy*.

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

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

4. 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 that access to information and information systems is limited to authorized users.

.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.