Data Classification and Security Policy

Kansas State University

Submitted to: IRMC on June 19, 2008
Submitted by: Harvard Townsend, Chief Information Security Officer
Date last modified: October 14, 2008
Send comments to: harv@k-state.edu and lcarlin@k-state.edu

I. Purpose

Data and information are important assets of the university and must be protected from loss of integrity, confidentiality, or availability in compliance with university policy and guidelines, Board of Regents policy, and state and federal.

II. Policy

All University Data should be classified according to the K-State Data Classification Schema and protected according to K-State Data Security Standards.

III. Data Classification Schema

Three levels of data classification are defined based on how the data is used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data is typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. For example, a student information system will contain a student's directory information as well as their social security number. Consequently, the classification of the most sensitive data element in a data collection will determine the data classification of the entire collection.

K-State Data Classifications:

A. ***Public*** – Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the University, affiliates, or individuals. Public data generally has a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:
   - K-State's public web site
   - Directory information for students, faculty, and staff except for those who have requested non-disclosure (for example, per FERPA for students)
   - Course descriptions
   - Semester course schedules
   - Press releases

B. ***Internal*** – Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data is generally not made available to parties outside the K-State community. Unauthorized disclosure could adversely impact the University, affiliates, or individuals. Internal data generally has a low to moderate sensitivity. Examples include:
   - Financial accounting data that does not contain confidential information

- Departmental intranet
- Information technology transaction logs
- Electronic ID ("eID")
- Wildcat ID ("WID")
- Employee ID ("W0…" number) and position numbers
- Student educational records
- Directory information for students, faculty, and staff who have requested non-disclosure (for example, per FERPA for students)

C. ***Confidential*** – Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the University or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or University contracts. Confidential data has a very high level of sensitivity. Examples include:

- Social Security Number
- Student ID number (if it is the same as the Social Security Number)
- Credit card number
- Personal identity information[1]
- Passport number
- Personnel records
- Medical records

Proprietary Data – Data provided to Kansas State University by a third party, such as a corporation or government agency, is owned by the third party unless explicitly stated otherwise in the contractual agreement. Individuals managing or accessing proprietary data are responsible for complying with the requirements and security policies and procedures specified by the third party owner. The sensitivity of data is likewise defined by the third party owner.

IV. Data Security Standards

The following table defines recommended safeguards for protecting data and data collections based on their classification. Data security requirements for Proprietary Data are determined by the contracting agency and are therefore not included in the table below.

In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts. For example, credit card information (classified as confidential data) must be protected according the standards specified by the Payment Card

[1] Kansas Senate Bill 196 (http://www.kslegislature.org/bills/2006/196.pdf) defines personal identity data as: An individual's name (first name and last name, or first initial and last name) in combination with one or more of the following: a) Social Security Number, b) driver's license number or other government-issued identification card number, or c) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. For K-State's purposes, PII also includes ones name in combination with a passport number.

Industry Data Security Standards (PCI DSS - https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf). Other examples include data covered by HIPAA or FERPA (see section VII below).

Security Control Category	***Data Classification***		
	Public	*Internal*	*Confidential*
Access Controls	No restriction for viewing. Authorization required for modification Data Steward grants permission for modification, plus approval from Data Manager	Viewing and modification restricted to authorized individuals Data Steward grants permission for access, plus approval from Data Manager Authentication and authorization required for access	Viewing and modification restricted to authorized individuals Data Steward grants permission for access, plus approval from Data Manager Authentication and authorization required for access Confidentiality agreement required
Copying/Printing (applies to both paper and electronic forms)	No restrictions	Data should only be printed when there is a legitimate need Copies must be limited to individuals with a need to know Data should not be sent to an unattended printer or left sitting on a printer	Data should only be printed when there is a legitimate need Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement Data should not be sent to an unattended printer or left sitting on a printer Copies must be stamped with “Confidential” or have a cover sheet indicating “Confidential”
Network Security	May reside on a public network	Protection with a firewall required	Protection with a firewall using “default deny” ruleset required

Security Control Category	***Data Classification***		
	Public	*Internal*	*Confidential*
	Protection with a firewall recommended IDS/IPS protection recommended Protection only with router ACLs acceptable	IDS/IPS protection required Protection with router ACLs optional Service should not be visible to entire Internet, but can be if necessary May be in a shared network server subnet with a common firewall ruleset for the set of servers	IDS/IPS protection required Protection with router ACLs optional Servers storing the data cannot be visible to the entire Internet Must have a firewall ruleset dedicated to the system The firewall ruleset should be reviewed periodically by an external auditor
System Security	Follows general best practices for system management and security Host-based software firewall recommended	Must follow University-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended	Must follow University-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended
Physical Security	System must be locked or logged out when unattended Secure Data Center recommended	System must be locked or logged out when unattended Secure Data Center recommended System must be in a secure location	System must be locked or logged out when unattended Must be located in a Secure Data Center Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access	No restrictions	Restricted to local	Restricted to local

Security Control Category	***Data Classification***		
	Public	*Internal*	*Confidential*
		network or general K-State Virtual Private Network (VPN) service Remote access by third party for technical support limited to authenticated, temporary access via dial-in modem or secure protocols over the Internet	network or secure VPN group Two-factor authentication recommended Remote access by third party for technical support not allowed
Storage	Storage on a secure server recommended Storage in a secure Data Center recommended	Storage on a secure server recommended Storage in a secure Data Center recommended Should not store on an individual's workstation	Storage on a secure server required Storage in Secure Data Center required Must not store on an individual's workstation Must not store on a mobile device (e.g. a laptop computer) AES Encryption required with 192-bit or longer key
Transmission	No requirements	No requirements	Encryption required (for example, via SSL or secure file transfer protocols) Cannot transmit via e-mail unless encrypted and secured with a digital signature
Backup/Disaster Recovery	Data should be backed up daily	Daily backups required Off-site storage recommended	Daily backups required Off-site storage in a secure location required Encrypted backups

Security Control Category	***Data Classification***		
	Public	*Internal*	*Confidential*
			recommended
Media Sanitization	*If system will be re-used:* Re-format hard drive(s) *If system will not be re-used:* no requirements	*If system will be re-used:* Overwrite data at least once so it is not recoverable *If system will not be re-used:* Overwrite or destroy (e.g. degauss) data so is not recoverable, or physically destroy the media	*If system leaving the institution:* Physically destroy the media *If system will be re-used internally:* Overwrite data three times or more so it is not recoverable (US DoD 5220.22-M (8-306./E) standard) *If system will not be re-used:* Physically destroy the media
Training	General security awareness training recommended System administration training recommended	General security awareness training required System administration training required Data security training recommended	General security awareness training required System administration training required System administrators should pass a criminal background check Data security training required Applicable policy and regulation training required
Audit Schedule	As needed	As needed	Annual

Note: the table above is adapted from the University of Missouri-Columbia Information & Access Technology Services data classification system: (http://iatservices.missouri.edu/security/data-classification/)

V. Roles and Responsibilities

Everyone with any level of access to University Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. The following roles have specific responsibilities for protecting and managing University Data and Data Collections.

A. ***Chief Data Steward*** – Senior administrative officers of the university responsible for overseeing all information resources (e.g., the Provost, Vice President for Administration and Finance, and Vice President for Institutional Advancement)

B. ***Data Steward*** – Deans, associate vice presidents, and heads of academic, administrative, or affiliated units or their designees with responsibility for overseeing a collection (set) of University Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, appointing Data Managers for each University Data collection, and ensuring compliance with K-State's data classification and security policies for all data for which they have responsibility.

C. ***Data Stewards Council*** – A group of Data Stewards appointed by the Chief Data Stewards and Vice Provost for Information Technology Services to maintain the data classification schema, define University Data collections, assign a Data Steward to each, and resolve data classification or ownership disputes.

D. ***Data Manager*** – Individuals authorized by a Data Steward to provide operational management of a University Data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.

E. ***Data Processor*** – Individuals authorized by the Data Steward and enabled by the Data Manager to enter, modify, or delete University Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.

F. ***Data Viewer*** – Anyone in the university community with the capacity to access University Data but is not authorized to enter, modify, or delete it.

G. ***Chief Information Security Officer*** – Provides advice on information and information technology security; monitors network, system, and data security; and coordinates the University's response to data security incidents.

H. ***Internal Audit Office*** – Performs audits for compliance with data classification and security policy and standards.

Note: The above roles and responsibilities are adapted from George Mason University's Data Stewardship Policy (http://www.gmu.edu/facstaff/policy/newpolicy/1114gen.html).

VI. Definitions

ACL – Access Control List; a set of rules in a network device, such as a router, that controls access to segments of the network. A router with ACLs can filter inbound and/or outbound network traffic similar to a firewall but with less functionality.

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.

Authorization – granting access to resources only to those authorized to use them.

Availability – Ensures timely and reliable access to and use of information.

Confidentiality – Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Criticality – Indicates the data's level of importance to the continuation of normal operation of the institution, or for compliance with law. The more critical the data, the greater the need to protect it.

Firewall – A specialized hardware and/or software system with stateful packet inspection that filters network traffic to control access to a resource, such as a database server, and thereby provide protection and enforce security policies. A router with ACLs is not considered a firewall for the purposes of this document.

IDS – Intrusion Detection System; a system that monitors network traffic to detect potential security intrusions. Normally, the suspected intrusions are logged and an alert generated to notify security or system administration personnel.

Integrity – Guards against improper modification or destruction of information, and ensures non-repudiation and authenticity.

IPS – Intrusion Prevention System; an IDS with the added ability to block malicious network traffic to prevent or stop a security event.

Secure Data Center – A facility managed by full-time IT professionals for housing computer, data storage, and/or network equipment with 24x7 auditable restricted access, environmental controls, power protection, and firewall protection.

Sensitivity – Indicates the required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or on one's reputation or competitive position. The more sensitive the data, the greater the need to protect it.

University Data – Any data related to Kansas State University ("University") functions that is 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.

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.

VIII. Related Regulations, Policies and Procedures

Federal Legislation and Guidelines

A. Family Educational Rights and Privacy Act of 1974 (FERPA - http://www.k-state.edu/registrar/ferpa/index.htm)
B. Health Insurance Portability and Accountability Act of 1996 (HIPAA - http://www.hhs.gov/ocr/hipaa/)

C. Gramm-Leach-Bliley Act (GLBA - http://www.ftc.gov/privacy/privacyinitiatives/glbact.html)
D. Electronic Communications Privacy Act of 1986 (ECPA - http://cio.doe.gov/Documents/ECPA.HTM)
E. NIST Publication 800-88 "Guidelines for Media Sanitization" (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)
F. NIST Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories" (http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf)
G. All NIST Special Publications 800 Series on Security (http://csrc.nist.gov/publications/nistpubs/)

State of Kansas

H. Kansas Information Technology Architecture Version 11 (http://www.da.ks.gov/itec/Architecture.htm)
I. Information Technology Policy 4010 – Technical Architecture Compliance Requirements (http://www.da.ks.gov/itec/Documents/ITECITPolicy4010.htm)
J. Senate Bill 196 on protecting personal identity information (http://www.kslegislature.org/bills/2006/196.pdf)
K. Information Technology Policy 8000 – Development of a Data Administration Program (http://www.da.ks.gov/itec/Documents/ITECITPolicy8000.htm)
L. State of Kansas Default Information Technology Security Requirements published by ITEC, March 2006 (http://www.da.ks.gov/itec/Documents/ITECITPolicy7230A.pdf). These do not directly apply to K-State, but offer good guidelines for data security controls and represent minimum standards required of non-Regents state agencies.

Kansas State University Policies

M. Collection, Use, and Protection of Social Security Numbers (http://www.k-state.edu/policies/ppm/3495.html)
N. Information Resource Management Policy (http://www.k-state.edu/policies/ppm/3425.html)
O. Information Security Plan (http://www.k-state.edu/policies/ppm/3415.html)
P. Protecting Sensitive Data by Desktop Search Products (http://www.k-state.edu/policies/ppm/3485.html)
Q. Research Data Retention, Records Retention, and Disposition Schedule (http://www.k-state.edu/policies/ppm/7010.html#.440)
R. Security for Information, Computing, and Network Resources (http://www.k-state.edu/policies/ppm/3430.html)

Other

S. Payment Card Industry Data Security Standard (PCI DSS) (https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf