FSCOT Agenda

Feb. 20th, 2007

FSCOT Meeting
Feb. 20th, 2007 1:00pm – 2:30pm
Location: Hale Library – Room 503 Deans Conference Room
Polycom IP address: 129.130.36.1 (for Salina call in)

Guest: none

Attachment 1: Proposed Data Classification and Security Policy and Standards

.1. New Business? Agenda additions?

.2. Old Business – discussion?

.3. Update memo from Dr. Gould about last week discussion items :
SPAM Issues
Placing School Holidays on the Oracle calendar.
Outsourcing Email
Email "forwarding" issues.

.4. Proposed Data Classification and Security Policy and Standards

.5. MS VISTA and Trend Micro Antivirus Malware software.

.6. Student Textbook Policy (potential)
Student Senate's University Relations Committee - Zimmerman

.7. Email Bounces – report from IT.

.8. AVPAST Search Committee status

.9. Daylight Savings Time issues.

.10. Server Storage Space – dilemma for IT
~250 MB left on SAN

.11. Request for faculty representative on the ePortfolio committee.

.12. Change to eID policy (interim statement) Policy 3450
Withdraw Central Data Retention policy.

.13. Zombie Computers – put you in jail.
Resulting and ongoing investigation

.14. Upcoming policies for review
Mobile Device Security
Data Classification

.15. Password length issue – why 7-8 characters

.16. InfoTech Tuesday
Problem – how to get people to read.
Example – the number of articles warning about VISTA.
Review some high points.

.17. Any "for the good of the University" items or last minute discussions?

.18. Adjournment

Attachment 1

DRAFT

Proposed Data Classification and Security Policy and Standards

Kansas State University

Submitted to: IRMC on November 16, 2006
Submitted by: Harvard Townsend, Interim IT Security Officer
Lynn Carlin, Special Projects Assistant to the Provost and Dean of Libraries
Date last modified: November 16, 2006
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 laws. A data classification system serves as a foundation for protecting university data assets.

II. Definitions

Availability- Ensuring timely and reliable access to and use of information.

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

Criticality – an indicator of the data's level of importance to the continuation of normal operation of the institution, or for compliance with law. If the data were unavailable, how would it impact the ability of Kansas State University to carry out its mission or to comply with regulations? The more critical the data, the greater the need to protect it.

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

Sensitivity – an indicator of the required level of protection from unauthorized disclosure, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. That 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 stored on Kansas State University information technology systems, maintained by faculty staff, or students, or related to institutional processes on or off campus.

III. Policy

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

IV. Data Classification Schema

Five levels of data classification are defined based on the 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 approved for distribution to the public without restriction. It can be freely distributed without potential harm to the University, affiliates, or individuals. This data classification 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
   - Student directory information for those who have not requested non-disclosure per FERPA
   - Employee contact information
   - eID
   - 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. It is generally not made available to parties outside the K-State community. Unauthorized disclosure could adversely impact the University, affiliates, or individuals. This data classification generally has a low to moderate sensitivity. Examples include:
   - Financial accounting data that does not contain confidential information
   - Departmental intranet
   - Library transactions
   - Information technology transaction logs

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, ethical, 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. This data classification has a high level of sensitivity. Examples include:
   - Student educational records
   - Student directory information when the student has requested non-disclosure per FERPA
   - Employee ID number
   - Personnel records
   - Medical records
   - Human subjects research data
   - Encryption keys
   - Biometric identifiers

D. ***Personal Identity*** – An individual's name or eID 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, c) passport number and country or visa number, or d) account number or credit or debit card number along with any required security code, access code, or password that provides access to that account. Unauthorized disclosure could result in identity theft and/or have a significant adverse impact on an individual or the University's reputation. This data classification has a high level of sensitivity. Examples include:

- Social Security Number
- Credit card number
- Passport number
- eID password
- Digitized signatures

E. ***National Security Interest (NSI) Data*** – Data that has been classified by a third party, such as a government agency, as having the potential to impact national security. Individuals managing or accessing NSI data are responsible for complying with the requirements and security procedures of levels 1, 2, and 3 of the National Security Decision Directives and/or other federal government directives for classified data or systems as specified by the source agency. The sensitivity of data in this classification is defined by the sponsoring agency.

V. Data Security Standards

The following table defines requisite safeguards for protecting data based on its classification.

Data security requirements for National Security Interest Data are determined by the contracting agency. An audit of compliance with the requirements in the following table must be performed according to the schedule listed in the table.

	Public	*Internal*	*Confidential*	*Personal Identity*
Access Controls	No restriction for viewing. Authentication required for modification Data Steward grants permission for modification, plus approval from supervisor	Viewing and modification restricted to authorized individuals Data Steward grants permission for access, plus approval from supervisor Authentication required for access	Viewing and modification restricted to authorized individuals Data Steward grants permission for access, plus approval from supervisor Authentication required for access Confidentiality agreement required	Viewing and modification restricted to authorized individuals Data Steward grants permission for access, plus approval from supervisor Authentication required for access Confidentiality agreement required
Copying/Printing	No restrictions	Data should only be printed when there is a	Data should only be printed when there is a	Data should only be printed when there is a

	Public	*Internal*	*Confidential*	*Personal Identity*
		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	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"	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 recommended IDS/IPS protection recommended Protection only with router ACLs acceptable	Protection with a firewall required IDS/IPS protection required Protection only with router ACLs not acceptable Service should not be visible to entire Internet, but can be if necessary May be in a shared network server zone with a common firewall ruleset for the set of servers	Protection with a firewall using "default deny" ruleset required IDS/IPS protection required Protection only with router ACLs not acceptable 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	Protection with a firewall using "default deny" ruleset required IDS/IPS protection required Protection only with router ACLs not acceptable 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

	Public	*Internal*	*Confidential*	*Personal Identity*
			reviewed by an external auditor periodically	reviewed by an external auditor periodically
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 required	Must follow University-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS required
Physical Security	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 Secure Data Center recommended	Access monitored and limited to authorized individuals 24x7 All physical access must be logged System must be locked or logged out when unattended Secure Data Center required	Access monitored and limited to authorized individuals 24x7 All physical access must be logged System must be locked or logged out when unattended Secure Data Center required
Remote Access	No restrictions	Restricted to local network or general K-State Virtual Private Network (VPN) service Remote access by third party for technical support limited to authenticated, temporary access	Restricted to local network or secure VPN group Two-factor authentication recommended Remote access by third party for technical support not allowed	Restricted to local network or secure VPN Two-factor authentication required Remote access by third party for technical support not allowed

	Public	*Internal*	*Confidential*	*Personal Identity*
		via dial-in modem or secure protocols over the Internet		
Storage	No requirements	Storage on a secure server recommended Storage in a secure Data Center recommended Should not store data on an individual's workstation	Storage on a secure server in a secure Data Center required. Must not store on an individual's workstation Must be encrypted if stored on a mobile device Encryption recommended	Storage on a secure server in a secure Data Center required. Must not store on an individual workstation Must not store on a mobile device (e.g. a laptop computer) Encryption required
Transmission	No requirements	No requirements	Secure protocols required Cannot transmit via e-mail	Secure protocols required Cannot transmit via e-mail
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 recommended	Daily backups required Off-site storage in a secure location required Encrypted backups required
Data Disposal	*If system will be re-used:* 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 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	*If system will be re-used:* Overwrite data three times or more so is not recoverable *If system will not be re-used:* Overwrite or destroy (e.g. degauss) data so is not recoverable, or physically	*If system will be re-used:* Overwrite data three times or more so is not recoverable *If system will not be re-used:* Physically destroy the media

	Public	*Internal*	*Confidential*	*Personal Identity*
		media	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 Data security training required Applicable policy and regulation training required	General security awareness training required System administration training required Data security training required Applicable policy and regulation training required
Audit Schedule	As needed	As needed	Annual	Semi-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/)

VI. 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.

A. ***Data Steward*** – Senior administrative officers, deans, department heads, directors, or managers responsible 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: classifying data under their control, granting data access permissions, appointing Data Administrators for each University Data set, serving on the Data Resource Stewards Council, and ensuring compliance with K-State's data classification and security system for all data for which they have responsibility.

B. ***Data Resource Stewards Council*** – A group of Data Stewards appointed by the Vice Provost of Academic Services and Technology to maintain the data classification schema, define University Data sets, assign a Data Steward to each, and resolve data classification or ownership disputes.

C. ***Data Administrator*** – Individuals authorized by a Data Steward to provide operational management a University Data set. The Data Administrator will maintain documentation pertaining to the data set (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.

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

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

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

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

H. ***Information Technology Assistance Center (iTAC)*** – Provides training and awareness in data classification and security policy and standards to the campus community.

I. ***Division of Human Resources*** – Provides training and awareness in data classification and security policy and standards to new employees.

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).

VII. Related Regulations, Policies and Procedures

Federal Legislation

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)

Kansas State University Policies

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