FSCOT Agenda
Tuesday, October 21, 2008
3:30 p.m - Bluemont 16e
Polycom IP Address 129.130.117.247

Approval of notes for September 16, 2008 meeting.

1. Report on iTunes U Progress
2. Discussion of IT Needs Assessment Report – Next Steps (http://upgrade.k-state.edu/results/)
3. Report on Policy Discussions IRMC Meeting, 10/16/08 – Next Steps (See Attached Draft Policies)

Next Scheduled FSCOT Meeting, Tuesday, November 4, 2008.

# Security Incident Reporting and Management Policy for Kansas State University

*Author*: Harvard Townsend, Chief Information Security Officer
*Date last modified*: October 14, 2008

## I. Purpose

This policy governs the actions required of University personnel reporting or responding to security incidents involving K-State information and/or information technology resources to insure effective and consistent reporting and handling of such events.

## II. Scope

This policy applies to all University personnel, units, and affiliates using University IT resources or data.

## III. Policy

All members of the University community are responsible for reporting known or suspected information or information technology security incidents.

All security incidents at K-State must be promptly reported to K-State's Chief Information Security Officer (CISO) and other appropriate authority(ies) and handled appropriately based on the type and severity of the incident in accordance with K-State security incident management policies and procedures.

All individuals involved in reporting or investigating a security incident are obliged to maintain confidentiality, unless the Vice Provost for Information Technology Services authorizes information disclosure in advance.

Handling of security incidents involving confidential data will be overseen by an Executive Incident Management Team and may have additional legal, policy, and/or contractual requirements for handling the incident and notifying affected parties.

## IV. Definitions

A *security incident* is any real or suspected event that may adversely affect the security of K-State information or the systems that process, store, or transmit that information.

Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities

- Denial of Service attack
- Web site defacement
- Violation of a K-State security policy
- Security weakness such as an un-patched vulnerability

See “Incident Categories” below for more examples.

The *Executive Incident Management Team* will oversee the handling of security incidents involving confidential data (*e.g.,* personal identity information). This team will have authority to make decisions related to the incident and to notify appropriate parties. The team will consist of:

- Senior administrator for the affected unit
- Vice Provost for IT Services
- Chief Information Security Officer
- Representative from the Office of the University Attorney
- Assistant Vice President for Media Relations
- Others as needed (for example, K-State Police for criminal incidents)

## V. Reporting Security Incidents

Any member of the K-State community who suspects the occurrence of a security incident must report incidents through the following channels:

- All suspected high severity events as defined in the incident classification system, including those involving possible breaches of personal identity data, should be reported directly to the Chief Information Security Officer as quickly as possible by phone, e-mail, or in person.

All other suspected incidents must also be reported to the Chief Information Security Officer or by sending e-mail to abuse@k-state.edu. These incidents may be first reported to departmental IT support personnel or the unit’s Security Incident Response Team (SIRT) representative who can then contact the Chief Information Security Officer.

## VI. Incident Classification System

Security incidents will be classified according to incident categories and severity of incident.  Incident response will be based on classification.

### A. *Incident Categories*

The following categories will be used to describe IT security incidents at Kansas State University. A single incident may have several different categories.

The examples listed in each category are not meant to be exhaustive.

a. *Confidential data exposure*
- Social Security Numbers with or without names
- Credit Card information
- Identity theft

- Other

b. *Criminal activity/investigation*
  - Subpeona, search warrant, or other court order
  - Litigation hold request (ala e-Discovery)
  - Online theft, fraud
  - Threatening communication
  - Child pornography
  - Physical theft, break-in

c. *Denial of Service*
  - Single or distributed (DoS or DDoS)
  - Inbound or outbound

d. *Digital Millennium Copyright Act (DMCA) violation*
  - Official DMCA notification from copyright owner or legal representative
  - Illegal distribution of copyrighted or licensed material (movies, music, software, games)
  - Illegal possession of copyrighted or licensed material

e. *Malicious code activity*
  - Worm, virus, Trojan
  - Botnet
  - Keylogger
  - Rootkit

f. *Policy violation*
  - K-State policy violation
  - Violation of student code of conduct
  - Personnel action/investigation

g. *Reconnaissance activity*
  - Port scanning
  - Other vulnerability scanning
  - Unauthorized monitoring

h. *Rogue server or service*
  - Rogue file/FTP server for music, movies, pirated software, etc.
  - Phishing scam web server
  - Botnet controller

i. *Spam source*
  - Spam relay
  - Spam host
  - K-State computer on a block list

j. *Spear Phishing*
  - Scam e-mail targeting a relatively large number of K-State e-mail addresses

k. *Unauthorized access*
  - Abuse of access privileges
  - Unauthorized access to data

- Unauthorized login attempts
- Brute force password cracking attempts
- Stolen password(s)

l. *Un-patched vulnerability*

- Vulnerable operating system
- Vulnerable application
- Vulnerable web site/service
- Weak or no password on an account

m. *Web/BBS defacement*

- Defacement of web site
- Inappropriate post to BBS, wiki, blog, etc.
- Redirected web site

n. *No Incident*

- When investigation of suspicious activity finds no evidence of a security incident

### B. *Incident Severity*

The severity of incident is a subjective measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

- Scope of impact – how many people, departments, or systems does it affect?
- Criticality of the system or service – how important is it to the continuing operation of the institution? What would be the impact on the business, either functional or financial, if this system or service were unavailable or corrupted?
- Sensitivity of the information stored on or accessed through the system or service – does it contain confidential data, such as personal identity information or credit card information?
- Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems off campus?

Security incidents will be classified by four categories of incident severity – high, medium, low, and NA ("Not Applicable").

a) *High*

The severity of a security incident will be considered "high" if *any* of the following conditions exist:

- Significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)

- Threatens confidential data (for example, the compromise of a server that contains credit card numbers or names with social security numbers)
- Adversely impacts an enterprise system or service critical to the operation of a major portion of the university (for example, e-mail, student information system, financial information system, human resources information system, learning management system, Internet service, and a major portion of the campus network)
- Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
- Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

High severity incidents require an immediate response and focused, dedicated attention by the CISO and other appropriate University officials and IT security staff until remediated. These incidents also have extensive notification and reporting requirements, as outlined in the table below. A Post-Incident Report is required. If the incident involves the possible exposure of personal identity data, it may require notification of individuals according to state of Kansas law (Senate Bill 196 that protects personal information of Kansas citizens).

b) *Medium*

The severity of a security incident will be considered "medium" if *any* of the following conditions exist:

- Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
- Adversely impacts a non-critical enterprise system or service
- Adversely impacts a departmental system or service, such as a departmental file server
- Disrupts a building or departmental network
- Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruptions

Medium severity incidents require a quick response by appropriate personnel, usually from the affected unit, who have primary responsibility for handling the incident. Notification requirements are outlined in the table below. A Post-Incident Report is not required unless requested by the Vice Provost for IT Services or other appropriate administrator.

c) *Low*

Low severity incidents have the following characteristics:

- Adversely impacts a very small number of systems or individuals
- Disrupts a very small number of network devices or segments
- Has little or no risk of propagation, or cause minimal disruption or damage in their attempt to propagate

Since a single compromised system can "wake up" and negatively affect other systems at any time, appropriate personal (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day. Notification requirements are outlined in the table below. A Post-Incident Report is not required unless requested by the Vice Provost for IT Services.

d) *NA* ("Not Applicable")
This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found. This usually corresponds to the incident category, "No Incident."

The following table summarizes incident severity categories and the requirements of each.

| *Incident Severity* | *Characteristics (one or more condition present determines the severity)* | *Response Time* | *Incident Manager* | *Who to Notify* | *Post-Incident Report Required* |
|---|---|---|---|---|---|
| **High** | **1)** Significant adverse impact on a large number of systems and/or people<br>**2)** Threatens confidential data<br>**3)** Adversely impacts a critical enterprise system or service<br>**4)** Significant and immediate threat to human safety<br>**5)** High probability of propagating to a large number of other systems on or off campus and causing significant disruption | Immediate | Chief Information Security Officer or an Executive Incident Management Team | **1)** Chief Information Security Officer<br>**2)** Vice Provost for IT Services<br>**3)** Unit administrator (VP, Provost, Dean, etc.)<br>**4)** Unit head<br>**5)** SIRT representative<br>**6)** Departmental security contact<br>**7)** Technical support for affected device<br>**8)** If confidential data affected, notify the victims, President's office and the CIO of the Kansas Board of Regents | Yes |
| **Medium** | **1)** Adversely impacts a moderate number of systems and/or people<br>**2)** Adversely impacts a non-critical enterprise system or service<br>**3)** Adversely impacts a departmental scale system or service<br>**4)** Moderate risk of propagating and causing further disruption | 4 hours | Appointed by unit head | **1)** Chief Information Security Officer<br>**2)** Unit head<br>**3)** SIRT representative<br>**4)** Departmental security contact<br>**5)** Technical support for affected device | No, unless requested by Vice Provost for IT Services or other appropriate administrator |
| **Low** | **1)** Adversely impacts a very small number of non-critical individual systems, services, or people<br>**2)** Little risk of propagation and further disruption | Next business day | Technical support for affected device | **1)** Chief Information Security Officer<br>**2)** SIRT representative<br>**3)** Departmental security contact | No |

| | |
|---|---|
| **NA** | “Not Applicable” – used for suspicious activities which upon investigation are determined not to be an IT security incident. |

## VII. Related K-State and State of Kansas Policies and Procedures

- Security Incident Management Procedures for Kansas State University (DRAFT)
- Security for Information, Computing and Network Resources - http://www.k-state.edu/policies/ppm/3430.html
- Information Technology Usage Policy - http://www.k-state.edu/policies/ppm/3420.html
- Information Security Plan - http://www.k-state.edu/policies/ppm/3415.html
- Policy on Collection, Use, and Protection of Social Security Numbers - http://www.k-state.edu/policies/ppm/3495.html
- Electronic Mail Policy - http://www.k-state.edu/policies/ppm/3455.html
- Wireless Local Area Network Policy - http://www.k-state.edu/policies/ppm/3480.html
- Procedures for removing compromised computers from the network - http://www.k-state.edu/infotech/security/procedures/compromised.html
- Microsoft Windows Computer Forensics at Kansas State University - http://www.k-state.edu/infotech/security/events/20071031/WindowsForensicsProcedures11-27-07.pdf
- Student Conduct Code - http://www.k-state.edu/osas/conductcode.htm
- Prohibited Use of Recreation Software - http://www.k-state.edu/policies/ppm/3490.html
- Data Classification and Security Policy and Standards (DRAFT) - http://www.k-state.edu/committees/irmc/draftpolicy/index.htm
- K-State Procedure for Handling Notifications of Copyright Infringement - http://www.k-state.edu/infotech/security/procedures/DMCAnotice.html
- Retention of Records policies and procedures - http://www.k-state.edu/policies/ppm/3090.html
- K-State Security Incident Response Team (SIRT) - http://www.k-state.edu/infotech/security/SIRT
- Enterprise IT Security Reporting Protocols, State of Kansas IT Security Council, October 2007 – http://www.da.ks.gov/itec/itsec/ITSec_Reporting_Oct07.pdf
- Kansas IT Executive Council (ITEC) IT Enterprise Security Policy, ITEC policy 7320 - http://www.da.ks.gov/itec/Documents/itecitpolicy7230.htm
- Kansas Senate Bill 192 that requires notification of victims in a breach of personal identity information - http://www.kslegislature.org/bills/2006/192.pdf

## VIII. References

- Computer Security Incident Response Team (CSIRT) resources, CERT Coordination Center, Carnegie Mellon University Software Engineering Institute - http://www.cert.org/csirts/

  - “Handbook for CSIRTs” from CERT CC,” April 2003 – http://www.cert.org/archive/pdf/csirt-handbook.pdf
- EDUCAUSE/Internet2 Security Task Force Incident Notification Toolkit - http://www.educause.edu/DataIncdentNotividationToolkit/9320
- EDUCAUSE/Internet2 Security Task Force Confidential Data Handling Blueprint - https://wiki.internet2.edu/confluence/display/secguide/Confidential+Data+Handling+Blueprint
- National Institute of Standards and Technology (NIST) special publication 800-61 - “Computer Security Incident Handling Guide (DRAFT),” September 2007 – http://csrc.nist.gov/publications/drafts/sp800-61-rev1/Draft-SP800-61rev1.pdf
- Federal Information Processing Standards (FIPS) publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006 – http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
- Chapter 13, “Information security incident management,” in ISO 17799:2005 international security standard – “Code of practice for information security management.” This document is not available on the web – it has to be purchased.

## 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

[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.

***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 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.<br>Authorization required for modification<br>Data Steward grants permission for modification, plus approval from Data Manager | Viewing and modification restricted to authorized individuals<br>Data Steward grants permission for access, plus approval from Data Manager<br>Authentication and authorization required for access | Viewing and modification restricted to authorized individuals<br>Data Steward grants permission for access, plus approval from Data Manager<br>Authentication and authorization required for |

| ***Security Control Category*** | ***Data Classification*** | | |
|---|---|---|---|
| | *Public* | *Internal* | *Confidential* |
| | | | access<br>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<br>Copies must be limited to individuals with a need to know<br>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<br>Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement<br>Data should not be sent to an unattended printer or left sitting on a printer<br>Copies must be stamped with "Confidential" or have a cover sheet indicating "Confidential" |
| *Network Security* | May reside on a public network<br>Protection with a firewall recommended<br>IDS/IPS protection recommended | Protection with a firewall required<br>IDS/IPS protection required | Protection with a firewall using "default deny" ruleset required<br>IDS/IPS |

| ***Security Control Category*** | ***Data Classification*** | | |
|---|---|---|---|
| | *Public* | *Internal* | *Confidential* |
| | Protection only with router ACLs acceptable | Protection with router ACLs optional<br>Service should not be visible to entire Internet, but can be if necessary<br>May be in a shared network server subnet with a common firewall ruleset for the set of servers | protection required<br>Protection with router ACLs optional<br>Servers storing the data cannot be visible to the entire Internet<br>Must have a firewall ruleset dedicated to the system<br>The firewall ruleset should be reviewed periodically by an external auditor |
| *System Security* | Follows general best practices for system management and security<br>Host-based software firewall recommended | Must follow University-specific and OS-specific best practices for system management and security<br>Host-based software firewall required<br>Host-based software IDS/IPS recommended | Must follow University-specific and OS-specific best practices for system management and security<br>Host-based software firewall required<br>Host-based software IDS/IPS recommended |
| *Physical Security* | System must be locked or logged out | System must be locked or logged out when | System must be locked or |

| ***Security Control Category*** | ***Data Classification*** | | |
|---|---|---|---|
| | *Public* | *Internal* | *Confidential* |
| | when unattended<br>Secure Data Center recommended | unattended<br>Secure Data Center recommended<br>System must be in a secure location | logged out when unattended<br>Must be located in a Secure Data Center<br>Physical access must be monitored, logged, and limited to authorized individuals 24x7 |
| *Remote Access* | No restrictions | Restricted to local network or general K-State Virtual Private Network (VPN) service<br>Remote access by third party for technical support limited to authenticated, temporary access via dial-in modem or secure protocols over the Internet | Restricted to local network or secure VPN group<br>Two-factor authentication recommended<br>Remote access by third party for technical support not allowed |
| *Storage* | Storage on a secure server recommended<br>Storage in a secure Data Center recommended | Storage on a secure server recommended<br>Storage in a secure Data Center recommended<br>Should not store on an individual's workstation | Storage on a secure server required<br>Storage in Secure Data Center required<br>Must not store on an individual's |

| ***Security Control Category*** | ***Data Classification*** | | |
|---|---|---|---|
| | *Public* | *Internal* | *Confidential* |
| | | | workstation<br>Must not store on a mobile device (e.g. a laptop computer)<br>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)<br>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<br>Off-site storage recommended | Daily backups required<br>Off-site storage in a secure location required<br>Encrypted backups recommended |
| *Media Sanitization* | *If system will be re-used:* Re-format hard drive(s) | *If system will be re-used:* Overwrite data at least once so it is not recoverable | *If system leaving the institution:* Physically destroy the media |

| ***Security Control Category*** | ***Data Classification*** | | |
|---|---|---|---|
| | *Public* | *Internal* | *Confidential* |
| | *If system will not be re-used:* no requirements | *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 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)<br>*If system will not be re-used:* Physically destroy the media |
| *Training* | General security awareness training recommended<br>System administration training recommended | General security awareness training required<br>System administration training required<br>Data security training recommended | General security awareness training required<br>System administration training required<br>System administrators should pass a criminal background check<br>Data security training required<br>Applicable policy and regulation training |

| ***Security Control Category*** | ***Data Classification*** | | |
|---|---|---|---|
| | *Public* | *Internal* | *Confidential* |
| | | | 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