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 s*ecurity 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 **2)** Threatens confidential data **3)** Adversely impacts a critical enterprise system or service **4)** Significant and immediate threat to human safety **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 **2)** Vice Provost for IT Services **3)** Unit administrator (VP, Provost, Dean, etc.) **4)** Unit head **5)** SIRT representative **6)** Departmental security contact **7)** Technical support for affected device **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 **2)** Adversely impacts a non-critical enterprise system or service **3)** Adversely impacts a departmental scale system or service **4)** Moderate risk of propagating and causing further disruption	4 hours	Appointed by unit head	**1)** Chief Information Security Officer **2)** Unit head **3)** SIRT representative **4)** Departmental security contact **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 **2)** Little risk of propagation and further disruption	Next business day	Technical support for affected device	**1)** Chief Information Security Officer **2)** SIRT representative **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.