IT Security Incident Reporting and Response Policy for Kansas State University

Date last modified: Oct. 14, 2008, rev. November 2008, recommended for approval by IRMC Nov. 20 and Faculty Senate President Dec. 30, 2008, approved by CEC Jan. 8. 2009

I. Purpose

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

II. Scope

This policy applies to all members of the University community, including students, personnel, units, and affiliates using University information technology 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) as outlined in Section V.

Incident response will be handled appropriately based on the type and severity of the incident in accordance with K-State security incident management table in Section VI and K-State's Security Incident Management Procedures. Handling of security incidents involving confidential data will be overseen by an Executive Incident Management Team.

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

The Vice Provost for Information Technology Services or designee must approve any exception to this policy or related procedures.

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

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

The *incident manager* is responsible for managing the response to a security incident as defined in the K-State security incident management table in Section VI.

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:

a. All suspected high severity events as defined in Section VI , including those involving possible breaches of personal identity data, must be reported directly to the Chief Information Security Officer as quickly as possible by phone (preferred), e-mail, or in person. If the Chief Information Security Officer cannot be reached, contact the Vice Provost for IT Services.

b. All other suspected incidents must also be reported to the Chief Information Security Officer. These incidents may be first reported to departmental IT support personnel, the unit's Security Incident Response Team (SIRT) representative, or the unit head who can then contact the Chief Information Security Officer. Reports should be made by sending email to abuse@k-state.edu (preferred) or by notifying the Chief Information Security Officer by phone, email, or in person.

VI. Responding to Security Incidents

Incident response will be managed based on the level of severity of the incident. The level of severity is a 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, the incident manager, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: – 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:

- Threatens significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)
- Poses a potential large financial risk or legal liability to the University
- 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, or 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

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 disruption

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 causes only minimal disruption or damage in their attempt to propagate

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.

The following table summarizes the incident severity categories, the responsible incident managers, and notification and reporting requirements. Detailed procedures for incident response and management are further defined in the K-State Incident Management Procedures.

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)** Potential large financial risk or legal liability to the University **3)** Threatens confidential data **4)** Adversely impacts a critical enterprise system or service **5)** Significant and immediate threat to human safety **6)** 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)** Disrupts a building or departmental network **5)** 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)** Disrupts a very small number of network devices or segments **3)** 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

- K-State Security Incident Management Procedures
- 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 requiring notification of victims in a breach of personal identity information – http://www.kslegislature.org/bills/2006/192.pdf

VIII. Questions

The Vice Provost for Information Technology Services (ITS) is responsible for this policy. Questions should be directed to the Chief Information Security Officer.