ITS POLICIES AND GUIDELINES
CATEGORY: Information Technology, Security, Privacy, Information Access & Management
STATUS: In Review

GUIDELINE TITLE: **Information Security Incident Response**

GUIDELINE PURPOSE:
The purpose of information security incident response is to:

- mitigate the effects caused by such an incident,
- protect the information resources of the University from future unauthorized access, use or damage, and
- ensure that Truman State University fulfills all of its obligations under University policy, and federal and state laws and regulations with respect to such incident.

Truman recognizes the need to follow established procedures to address situations that could indicate the security of the University's information assets may have been compromised. Such procedures include ensuring the appropriate level of University management becomes involved in the determination of actions implemented in response to an information technology security incident.

A standard University-wide approach to information security is important in order to protect the security of Truman's intellectual capital and to ensure that Information Security Incidents are handled properly, effectively and in a manner that minimizes the adverse impact to the University. Every user of any of Truman's information resources has responsibility toward the protection of the University's information assets; certain offices and individuals have very specific responsibilities.

APPLIES TO:
This policy is applicable to all University students, faculty, staff, and to all others granted use or custodianship of Truman State University information resources ("University Community").

CONTENTS:

GUIDELINE STATEMENT:
This guideline describes the procedures to be followed when a computer security incident is discovered to have occurred involving an Academic or Administrative Computing System operated by Truman State University, its faculty, students, employees, consultants, vendors or others operating such systems on behalf of Truman. It also describes the procedures to be followed when prohibited or restricted information residing on any computing or information storage device is, or may have been, inappropriately accessed, whether or not such device is owned by Truman. This policy outlines the procedures for decision-making regarding emergency actions taken for the protection of Truman's information resources from accidental or intentional unauthorized access, disclosure or damage.

Notification

A member of the University Community who becomes aware of an Information Security Incident should immediately:

1. Disconnect the compromised system and equipment from Truman's network.
2. Avoid making any updates or other modifications to software, data, or equipment involved or suspected of involvement with an Information Security Incident until after the Information Technology Services Office has completed its investigation and authorizes such activity.
3. Contact the Information Technology Services Office at (660) 785-4163

Investigation

When an Information Security Incident is reported, the University's Chief Information Officer will do the following:

1. The CIO will ask the ITS Technical Director to investigate the Information Security Incident. In order to minimize the impact of the Information Security Incident on the University and in order to complete a proper investigation, the ITS Technical Director has the authority to restrict information system access or operations to protect against unauthorized information disclosures. In order to complete the investigation, the ITS Technical Director may convene a preliminary fact-finding working group comprised of relevant business and technical personnel.
2. If the CIO concludes that applicable federal or state laws or regulations may have been violated, the CIO will notify the Office of the General Counsel, which will, in turn, notify law enforcement agencies if appropriate.
3. If the CIO concludes that there is a possibility of unauthorized access to restricted or prohibited information, or other sensitive information, the CIO will convene a Computer Incident Response Team.
4. If appropriate, the CIO will notify offices of the Deans and Vice Presidents with responsibility for areas affected by the Information Security Incident.

Computer Incident Response Team

Based on information provided by the ITS Technical Director and in consultation with the Office of the General Counsel the CIO will convene a Computer Incident Response Team (CIRT) to develop an appropriate Information Security Incident Response Plan (Plan). Depending on the circumstances of each situation, the CIO shall include in the CIRT representatives of some or all of the following offices:

- Office of the General Counsel
- Office of the Provost and Vice President for Academic Affairs
- IT Services
- Departments or schools directly affected by the Information Security Incident (including both the appropriate business and technical personnel)
- Other constituencies, as appropriate.

The CIRT will develop and execute communication and other action plans to ensure:

1. Appropriate action is taken in a timely manner, including reporting, notification and other communication of the Information Security Incident, as required by law or otherwise deemed appropriate.
2. Appropriate progress reports are made on the Information Security Incident and execution of the Plan, including to:
    - Office of the Provost and Vice President for Academic Affairs
    - Other impacted constituencies, as warranted by the situation

In carrying out this responsibility, the CIRT will ensure that important operational decisions are elevated to the appropriate levels to protect the fundamental interests of the University and others impacted by the incident. The CIO will also be responsible for documenting the deliberations and decisions of the CIRT as well as all actions taken pursuant to CIRT deliberations.

Report Preparation

The Information Technology Services Offices will be responsible for writing a final report on the incident and the ensuing investigation (Report), which summarizes findings regarding the Information Security Incident and, if appropriate, makes recommendations for improvement of related information security practices and controls. The Report will be distributed to the Provost and Vice President for Academic Affairs, and other appropriate University office(s), if any.

CONTACTS:

Responsible Executive:	Provost and Vice President for Academic Affairs
Responsible Office:	Information Technology Services
Contact:	Chief Information Officer 111 McClain 660-785-4163
APPROVED BY:	Truman State University President
APPROVED ON:	2013/XX/XX
EFFECTIVE ON:	2013/XX/XX
REVIEW/CHANGE HISTORY:	2010/06/03, 2011/02/03
REVIEW CYCLE:	As Needed

DEFINITIONS:

a. **Academic Computing System** — Any application, or information system, that directly or indirectly deals with or supports the University's primary mission of teaching, learning and research.

b. **Administrative Computing System** — Any application, or information system, that directly or indirectly deals with or supports financial, administrative, or other information that is an integral part of running the business of the University.

c. **Electronic Information Security Incident** — An Electronic Information Security Incident is defined as any real or suspected adverse event in relation to the security of computer systems, computer networks, electronic prohibited information or electronic restricted Information. Examples of incidents include:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Theft or other loss of a laptop, desktop, PDA, or other device that contains prohibited or restricted information, whether or not such device is owned by Truman.
- Unwanted disruption or denial of service.
- The unauthorized use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

d. **Information Security Incident** – An Electronic Information Security Incident or a Non-electronic Information Security Incident.

e. **Non−electronic Information Security Incident –** Real or suspected theft, loss or other inappropriate access of physical content, such as printed documents and files.

RELATED DOCUMENTS:

Laws:

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Title 18 of the U.S. Code)
Electronics Communications Privacy Act of 1986 (PL 99-474)

Computer Security Act of 1987 (PL100-235)
*USA Patriot Act of 200*1
Password Policy
Information Security Policy

KEYWORDS: