University of Illinois at Springfield

Security Incident Handling Procedure

1. Purpose

The purpose of this Procedure is to ensure consistency in the handling of security incidents that occur on computing resources, to help to contain the incident, and to preclude the inadvertent destruction of forensic data evidence.

2. Scope

This procedure is intended to be used by anyone who uses computing equipment owned by the University of Illinois at Springfield (UIS) and/or anyone who uses computing equipment that contains or processes sensitive data stewarded by UIS.

This process covers the necessary activities that must occur from the time that an incident is first suspected or discovered to the time that the equipment can be safely returned to production status.

3. Definitions

Security Incident:
A security incident is defined as a compromise of a computer or other electronic system by malicious or unintended activity. Included in this definition is the unintentional disclosure of sensitive data to an unauthorized party. This could be a result of physical theft, deliberate attack, or accidental disclosure through system management errors.

Sensitive Data:
Sensitive data is an ever growing list of personal identifiers. Essentially, any data object (word, code, ID number, etc.) that can be used to identify a person or access any secure accounts can be considered sensitive data. Social Security numbers, credit card numbers, passwords, University ID numbers (UINs), and mother's maiden names are typical examples of sensitive data. Some types of health and medical data, financial data, academic data, and employment data are also considered sensitive or confidential.

Standard Level Security Incidents:
Incidents of this type meet **ALL** of the following criteria:

* There is no sensitive data on the compromised computer [1]
* The primary user(s) of the compromised computer does(do) not have access to sensitive information [1]
* The compromised equipment is a desktop or laptop computer

High Level Security Incidents:
All incidents that are not Standard Level Security Incidents are High Level Incidents.

Incident Managers:
UIS Security Incidents are managed by the following:

Name	On-Campus Phone	Cell Phone	email address
Technology Support Center	(217) 206-6000	n/a	TechSupport@uis.edu
Director/IT Operations	(217) 206-7755	(217) 720-0256	ITSecurity@uis.edu

4. Actions

A. Initial Recognition of Incident:

STEPS	RESPONSIBLE PERSON	DESCRIPTION
1. Notify Technology Support Center (TSC)	The person who identifies or suspects a computer security incident.	Call (217) 206-7355 during normal operating hours. Call (217) 720-0256 at any other time.
2. Verify the symptoms of the incident	TSC Professional	Corroborate the behaviors identified by the person who discovered the incident
3. Contain the incident if necessary	TSC / User reporting incident	Determine if necessary to shutdown port or to remove the network cable from the affected computer(s).
4. Preserve the running state	TSC Professional	Do not power off the computer so that the running state is preserved. This is critical to performing any forensic investigations that may be warranted.
5. Document incident details	TSC Professional	Collect: - IP Address(es) - Computer Name - URL (if applicable) - Computer function (workstation, web server, file server, email server, etc) - OS & version/patch level - Known data types housed on machine - Description of problem

6. Contact Director/IT Operations	TSC Professional	Call (217) 206-7355 and/or send an email to ITsecurity@uis.edu
7. Identify incident type	Director/IT Operations	Classify incident as a Standard Level Security Incident or a High Level Security Incident
8. Next Steps	TSC Professional	Proceed to 4.B for Standard Level Incidents or 4.C for High Level Incidents

B. Standard Level Security Incidents:

STEPS	RESPONSIBLE PERSON	DESCRIPTION
1. Notify users	User reporting incident	Notify any affected users explaining outage. Include expected duration of outage.
2. Move computer*	TSC Professional	Move computer to TSC
3. Verify latest versions	TSC Professional	Boot the computer with a known clean image using external bootable media.
4. Copy user files	TSC Professional	Copy user files to clean storage media
5. Re-image computer	TSC Professional	Scratch and reinstall operating system from stored image
6. Update operating system	TSC Professional	Download and apply latest patches for the operating system
7. Install Anti-Malware software	TSC Professional	Install latest versions of anti-virus and anti-malware applications
8. Restore files	TSC Professional	Restore user files from storage media
9. Scan computer	TSC Professional	Run a full anti-virus/anti-malware scan to ensure no malware was restored via restored files
10. Return computer	TSC Professional	Return computer to user
11. Notify Director/IT Operations Director/IT Operations	TSC Professional	Notify Director/IT Operations that procedures are complete

C. High Level Incidents:

STEPS	RESPONSIBLE PERSON	DESCRIPTION
1. Notify users	TSC Professional	Send email explaining outage to appropriate user groups, include expected duration of outage.
2. Physical Security	TSC Professional	Ensure that the physical security of the affected computer(s) is preserved.
3. Assist the Director/IT Operations	User Department	Provide the necessary access and resources for the Director/IT Operations to investigate the incident
4. Perform damage assessment	Director/IT Operations	Determine if sensitive data was compromised, determine threat to the University, notify management if necessary
5. Rebuild computer(s)	TSC Professional	Once the Director/IT Operations give the approval, follow the Departmentally Addressable Incident Handling procedure (4.B in this document)

* Only University-owned computers will be cleaned by the TSC. The cleaning of privately owned computers is the responsibility of the owner. ITS will take measures to ensure that privately owned computers involved in a security incident cannot access University networks or resources until they are verified to be clean by the TSC.

6. Responsibilities

The Director/IT Operations is responsible for maintaining the referenced contact information, email addresses, phone numbers, and hyperlinks that are referenced within this document.

Specific responsibilities for carrying out procedures are listed in Section 4.

7. Implementation

This procedure is included in the Policies section of the Information Technology Services website: http://www.uis.edu/its/about/policies.html