

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 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 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.

University of Illinois at Springfield

Security Incident Handling Procedure

Incident Managers:

UIS Security Incidents are managed by the following:

| Name | On-Campus Phone | Cell Phone | email address |
|---------------------------|-----------------|--------------|---------------------|
| Technology Support Center | 6.6000 | | TechSupport@uis.edu |
| Security Officer | 6.7355 | 217.299.7722 | 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 6.6000 M-F, 8:30 – midnight, Sa 10 – 6, Su 1 - 9 217.299.7722 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. 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 |
| 5. Contact the Security Officer | TSC Professional | Call 6.7355 and/or send an email to ITsecurity@uis.edu |
| 6. Identify incident type | Security Officer | Classify incident as a Standard Level Security Incident or a High Level Security Incident |
| 7. Next Steps | TSC Professional | Proceed to 4.B for Standard Level Incidents or 4.C for High Level |

University of Illinois at Springfield

Security Incident Handling Procedure

| | | |
|--|--|-----------|
| | | 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 | Update anti-virus and anti-malware applications if necessary |
| 4. Update operating system | TSC Professional | Download and apply latest patches for the operating system |
| 5. Scan Computer | TSC Professional | Scan computer for malware |
| 6. Next Steps | TSC Professional | If computer is clean, proceed to step 13 (return computer) |
| 7. Copy user files | TSC Professional | Copy user files to storage media |
| 8. Re-image computer | TSC Professional | Scratch and reinstall operating system from stored image |
| 9. Update operating system | TSC Professional | Download and apply latest patches for the operating system |
| 10. Install Anti-Malware software | TSC Professional | Install latest versions of anti-virus and anti-malware applications |
| 11. Restore files | TSC Professional | Restore user files from storage media |
| 12. Scan computer | TSC Professional | Run a full anti-virus/anti-malware scan to ensure no malware was restored via restored files |
| 13. Return computer | TSC Professional | Return computer to user |
| 14. Notify Security Officer | TSC Professional | Notify Security Officer that procedures are complete |

University of Illinois at Springfield

Security Incident Handling Procedure

C. Campus Security 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 Security Officers | User Department | Provide the necessary access and resources for the Security Officers to investigate the incident |
| 4. Perform damage assessment | Security Officer | Determine if sensitive data was compromised, determine threat to the University, notify management if necessary |
| 5. Rebuild computer(s) | TSC Professional | Once the Security Officers 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 Security Officer 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>