Astronomy IT Department Incident Response Procedure

Policy

In the event of a possible security incident concerning ***sensitive institutional or personal data***, report the incident as follows:

1. **IMMEDIATELY CALL**, no matter what time of day or night or weekday or weekend or holiday, until you get to a human. Try in this order:

    a. Bob Lezotte at 812-219-9874
    b. UITS Support Center at 812-855-6789 (24x7)
    c. UITS Network Operations Center at 812-855-3699 (24x7)

    When you reach the Support Center or the Network Operations Center, ask staff to PAGE the University Information Security Office (UISO). A representative from UISO will then call you back.

    Please **ALSO REPORT** the incident yourself:

    - Send an email to it-incident@iu.edu outlining the incident details.

    Please **DO NOT** simply leave voicemail or send e-mail - please ensure you reach a human, because it is **CRITICAL** that we begin response procedures immediately.

2. Call the following departmental leadership, in the following order:

    1. Bob Lezotte, IT
        a. IT will provide information about the incident to the CPSO of the College
        b. IT will provide Information about the incident to the CTO of the College
    2. Prof. Caty Pilachowski, Chair

3. For incidents involving a compromised computer or other IT system or device:

    - **STEP AWAY** from the computer
    - **DO NOT** touch it, or take any other action until advised by the Information Policy and Security Offices.
    - **DO NOT** attempt to login, or alter the compromised system.
    - **DO NOT** power it off.
    - These actions will delete forensic evidence that may be critical to your incident

4. **DO NOT** discuss the incident with any other parties until you are authorized. This is critical to ensure that only accurate information is disseminated, rather than suppositions or guesses as to what happened.

Investigation and Coordination

The UIPO and UISO are charged with the investigation and coordination of incidents where the loss, corruption, inappropriate disclosure, or exposure of information assets is suspected. When the UIPO and /or UISO are notified, an Incident Team will be assembled to advise and assist in containing and limiting the exposure, in investigating the incident, in obtaining the appropriate approvals, and in handling notification to the affected individuals and agencies.

The organizational unit experiencing the incident is fully responsible for allocating the resources needed to lead and achieve an appropriate and timely resolution of the incident. The unit experiencing the incident "owns" the response to the incident. The UIPO and UISO will provide oversight and guidance to the process to ensure a consistent, efficient and thorough response, and to ensure that all necessary approvals are received.

For more information or information security incident management at IU, see: Information Security Incident Management.

Collecting information about IT related incidents

If you find yourself involved in an incident involving IT systems, collecting the following information (if possible, and **without using the system**) will be helpful in the ensuing investigation:

- IP address(es)
- Hostname(s)
- Operating system & version
- Manufacturer, model, & serial number
- Usernames of users and system administrators of the machine
- Approx. date/time of compromise, if known
- List of software installed
- Attack vector (if you know / suspect a particular program,/service)

The UISO has experienced and certified forensic engineers on staff in the event that an in-depth investigation is necessary. the time required to conduct an investigation will vary greatly from one incident to another; no two incidents are alike. Accurately Collecting all necessary information is essential to a forensic investigation, and must remain a higher priority than returning equipment within a designated time frame. While a two week minimum is usually reasonable, please understand that it is only an estimate.

Guiding IU Policy / Policies

- ISPP-26 Information and Information System Incident Reporting, Management, and Breach Notification

Supporting Documents