SoIC IT Privacy and Security Incident Response Policy

SoIC IT Security/Privacy Incident/Concern Response Policy

Much of this document's language has been taken from the official IU incident response pages at protect.iu.edu. That site should be consulted in all cases to ensure that current university policies and procedures are followed.

Immediately report any of the following to the University Information Policy Office (UIPO) and to the SoIC Director of Information Technology and to the SoIC Chief Information Privacy and Security Officer (Associate Director of IT):

- Suspected or actual security breaches of information – whether in printed, verbal, or electronic form – or of information systems used in the pursuit of the university's mission.
- Abnormal systematic unsuccessful attempts to compromise information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission.
- Suspected or actual weaknesses in the safeguards protecting information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission.

If you suspect that a machine may be compromised and you know that it stores or processes sensitive data, please step away from the computer and do not use the system. That means you should not do a network scan of the system, run antivirus software, patch the system, reboot, unplug any cables, nor power off the system. Two reasons are:

- Your actions may inadvertently trample over important evidence, including the modify, access, and create times of files that the attacker viewed or touched.
- Your actions may tip off the attacker to know that you are aware that the machine is compromised. He or she may take action to remove evidence or delete files.

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

1. **STEP AWAY** from the computer
   - DO NOT touch it, or take any action until advised by the Information Policy & 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.

2. **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:
   1. UISO directly at 812-855-UISO (8476) (business hours)
   2. UITS Network Operations Center at 812-855-3699 (24x7)
   3. UITS Support Center at 802-855-6789 (24x7)

When you reach the Support Center or Network Operations Center, ask staff to contact UITS Data Center Operations so that a PAGE can be sent to the University Information Security Office (UISO). A representative from UISO will then call you back.

Please **ALSO REPORT** the incident yourself, using one of the following methods:

- Use our online incident reporting form (authentication required).
- Send an email to it-incident@iu.edu outlining the incident details.

3. **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.
4. Begin writing a detailed description to be shared with the Incident Team: what made you suspect the incident, what you know happened thus far, information on the machine and the data affected, and what actions have been taken so far.
5. For production services such as web sites or applications, plan remedial action to restore service and when. Consider bringing up a new machine to host the site or posting a “down for maintenance” banner.

**NOTE:** take caution if restoring service from a backup - especially if you're uncertain when the compromise occurred. It's possible you could restore a backup snapshot taken after the compromise.

If you find yourself involved in an incident involving IT systems, collecting the following information (do this without using the system – information can be gathered from the SoIC Hardware Database by members of the IT and Facilities Groups) will be helpful in the ensuing investigation:

- IP address(es)
- Hostname(s)
- Operating system and version
- Manufacturer, model, and 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 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. SoIC is fully responsible for allocating the resources needed to lead and achieve an appropriate and timely resolution of the incident. SoIC "owns" the response to the incident. The UIPO and UIISO 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.

Other reportable incidents:
Suspected Phishing emails – May be forward with full headers to phishing@iu.edu
Email abuse, misuse or spam may be forwarded with full headers to it-incident@iu.edu
Non-emergency security incident or privacy concerns should be reported to it-incident@iu.edu

Definitions

**Breach**
the acquisition, access, use, or disclosure of information in a manner not permitted under existing law or university policy that compromises the security or privacy of the information (i.e. poses a significant risk of financial, reputational, or other harm to the individual and/or university).

**Health Information**
any information created, maintained or received, via any communication or record retention format, by any entity such as a provider, insurance plan, employer, or university that identifies an individual and any services regarding their health care or health payments relating to their past, present, or future health status.

**Information system**
a discrete set of information resources, procedures and/or techniques, organized or designed, for the classification, collection, accessing, use, processing, manipulation, maintenance, storage, retention, retrieval, display, sharing, disclosure, dissemination, transmission, or disposal of information. An information system can be as simple as a paper-based filing system or as complicated as a tiered electronic system.

**Security Incident**
the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Security incident also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, misrouting of mail, or compromise of physical security, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.