Incident Response Policy
IU SEC-04

Scope

Indiana University Health Sciences (IUHS)

All employees and faculty of IUHS, as well as vendors, contractors, partners, students, collaborators, and any others doing business or research with IUHS, will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving IUHS computers, technology systems, and/or data will also be subject to the provisions of this policy.

IUHS computing resources have been developed to encourage widespread access and distribution of data and information for the purpose of accomplishing the educational, clinical, and research missions of the school. This policy will not supersede any Indiana University developed policies but may introduce more stringent requirements than the university policy.

Policy Statement

1. The Chief Information Officer and Associate Vice President for Information Technology, Clinical Affairs IT Services, is responsible for all actions necessary to protect IUSM people, resources, data, and/or communications in the event of an information security incident involving an IUHS school.
2. The Chief Information Security Officer (CISO), Clinical Affairs IT Services, serves as the investigative and operational lead for the conduct of all IUHS security incident investigations. The CISO will be the primary authority for invoking incident response procedures for IUHS schools.

3. Various IUHS schools, departments and centers will provide core and adjunct members of the incident response team to assist the CISO during security incident investigations. All incident response team members will be assigned duties based on the circumstances of the incident.

4. IUHS personnel must immediately report the following:
   a. a security incident that involves unauthorized physical access to a building or secure location, physical threat, imminent danger, or personal safety issue to the IU Police Department;
   b. an actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by IU and/or IUHS schools; malicious alteration or destruction of data, information, or communications; unauthorized interception or monitoring of communications; and any deliberate and unauthorized destruction or damage of IT resources to the Indiana University IT Security Office (UISO) as outlined in university incident reporting procedures.

5. All communications with the media regarding an incident will be coordinated through the appropriate university Media Relations office.

---

**Reason for Policy**

The purpose of this policy is to outline the different responsibilities of the IUHS schools, and centers with regard to reacting and responding to various types of network and information security incidents that may occur within IUHS.

---

**Definitions**

*Security incidents* can generally be defined as "the act of violating an explicit or implied security policy." (Definition is taken from the Carnegie Mellon Computer Emergency Response Team Coordination Center Incident Reporting System Guidelines.)

An *IUSM security incident* is defined as an event that exposes IUHS-held data to unauthorized individuals and impacts or has the potential to impact negatively either patient safety or privacy, IUHS employee safety or privacy, or the reputation of IU.

The *Core incident response team* consists of those members of various IUHS offices, departments, and centers who will assist in the conduct of a major incident investigation.
Adjunct incident response team members are those members of various IUHS schools, departments and centers who have specific skills needed at times during incident investigations.

---

**Sanctions**

If it is suspected that this policy is not being followed, report the incident to a departmental manager or representative and the Chief Information Security Officer.

Any exceptions to this policy must be approved in advance by the CISO and the CIO, Clinical Affairs IT Services.

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of Indiana University Policy IT-02, Misuse and Abuse of Information Technology Resources.

---

**History**

1. IUSM SEC-04, 12 Nov 2004, original policy.
2. Revision, March 31, 2005: Added "Centers" to the following: Definitions section, Core Incident Response Team, and Adjunct Incident Response Team definitions.
3. Policy reviewed on February 24, 2011.
5. Policy scope edited, expanded to include “Health Sciences”, August 4, 2014.