Security Within the IUSM Research Community
IU SEC-07

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 and technology systems will also be subject to the provisions of this policy.

Policy Statement

1. As custodians of the research data, principal investigators are ultimately responsible for the security of that data. As such, the principal investigators will ensure that the security of the research data in their control is maintained by them and all involved in the research project commensurate with the requirements of current state and federal regulations as well as university and IUHS policy.
2. The organization supporting the principal investigator will ensure that an appropriate security plan is developed for computer systems and networks supporting research. The organization's security plan will be developed consistent with the requirements detailed in existing university and IUHS policy and procedures.

3. Principal investigators must immediately use existing university incident reporting channels to report situations where sensitive research data may have been inadvertently released.

---

**Reason for Policy**

Access to selected research data and their supporting computer systems must be restricted pursuant to the provisions of various university policies and in accordance with legal and ethical requirements. The possibility of premature or inappropriate disclosure of research data to unauthorized persons could lead to a loss of intellectual property rights or public misrepresentation of the purpose of the research. In addition, in order to ensure the integrity and viability of all research data, we must guard against the possibility that unauthorized persons could gain privileged access that would afford them the opportunity to modify the data.

This policy outlines the responsibilities researchers have when safeguarding research data. This policy will not supersede any Indiana University developed policies but may introduce more stringent requirements than the university policy.

---

**Definitions**

*Principal investigators* are defined as those individuals in the research community responsible for conducting research, obtaining research grants, etc.

*Research data* is that data used or developed by principal investigators and others in support of research activities.

---

**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 both the Chief Information Security Officer and the Associate Vice President for Information Technology, 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-08, 5 Apr 2005, first draft of policy.
2. Policy reviewed on February 24, 2011.
5. Policy scope edited, expanded to include Health Sciences, August 5, 2014