Electronic Mail Security Policy
IU SEC-06

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. Anyone who uses the IU Messaging System shall not use email as a form of communication for messages containing information classified by IU as CRITICAL, RESTRICTED or UNIVERSITY-INTERNAL unless the communication is protected by appropriate security measures (i.e., encryption).

2. The Chief Information Officer, Clinical Affairs IT Services, will approve the means for protecting the security of the electronic communication for IUHS.
3. Email shall not be used to conduct personal business involving any for-profit enterprise not tied to the university.

4. The IU Messaging System will not be used to propagate chain letters, spam, or any other form of junk mail.

5. IUSM email mailing lists must not be distributed to third parties for commercial purposes.

---

**Reason for Policy**

The purpose of this policy is to establish appropriate uses of electronic mail for communications. In addition, this policy informs the IUHS email user community how privacy and security apply to email, as well as the applicability of relevant policy and law. This policy is based upon Indiana University's Email Use policy. This policy will not supersede any Indiana University developed policies and procedures but may introduce more stringent requirements than the university policy.

---

**Definitions**

*Email* is defined as the Indiana University (IU) Messaging System for transmitting electronic (written) messages.

*IUSM email mailing lists* is defined as a list of official email addresses of IUSM personnel.

*Email user* is defined as any faulty, resident, student, or staff member who has been assigned an IU email address and/or who has access to the IU Messaging System.

Data is described as **CRITICAL** if the inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals.

Data is labeled **RESTRICTED** if, because of legal, ethical, or other constraints, the data may not be accessed without specific authorization, or only selective access may be granted.

Data is deemed **UNIVERSITY-INTERNAL** if the data may be accessed by eligible agents of the university, in the conduct of university business; access restrictions should be applied accordingly.

---

**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-06, 17 Nov 2003, first draft of policy.
2. Policy reviewed on February 24, 2011.
4. Policy review, minor revisions, August 8, 2013
5. Policy scope edited, data classifications added, scope expanded to include Health Sciences, August 5, 2014