Backup and Recovery Policy
IU SEC-03

Scope

Indiana University Health Sciences

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.

Federal and state regulations pertaining to the long-term retention of data (e.g., medical records, financial records, etc.) will be met using separate archive policy and procedures, determined by the managers of the information. Long-term archive requirements are beyond the scope of this policy. Finally, this policy only addresses backup and recovery of electronic data. Paper records are beyond the scope of this policy.

Policy Statement

1. Center, department, and practice plan managers are responsible for developing a backup and recovery plan to facilitate the proper protection of institutional data. The plan should include, but is not necessarily limited to, the following:
Identification of all critical data, applications, documentation, personnel, facilities, and other support items that would be necessary to perform essential tasks during a recovery period

- The data steward responsible for the department of organization's critical data
- The specific backup and recovery processes designed to restore the organization's critical data
- The backup scheme used (timeframe for full, incremental, etc.)
- Location for offsite storage of critical data. (Organizations will document the procedures for maintaining a current copy of the critical data and will determine the frequency of update to this offsite storage.)
- Documentation of the restoration process, including the procedures for the recovery from single-system or application failures, as well as for a total disaster scenario

2. Backup and recovery plans must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.

3. All critical information shall be placed on a networked file server for backup. It is recommended that no critical information, including Protected Health Information as defined by the Health Information Portability and Accountability Act (HIPAA), be permanently stored on workstations, laptops, or personal devices unless there is a business necessity and the data is backed up to an appropriate server.

4. Recovery procedures will be tested on a periodic basis; however, at a minimum, these procedures will be tested on an annual basis.

---

**Reason for Policy**

All electronic information considered of institutional value should be copied onto secure storage media on a regular basis (i.e., backed up) for disaster recovery and to facilitate business continuity. The purpose of this policy is to outline the minimum requirements regarding backing up and recovering information of institutional value for IUHS.

---

**Definitions**

*Managers* are defined as department chairs, center directors, or similarly responsible people who make decisions related to the business uses of their organization's information.

*Data Stewards* are those members of the IUHS community who have the primary responsibility for managing access to, and use of, particular information.
Institutional data is defined as specific data necessary for the conduct of the organization's business. Generally, commercially available applications and operating systems are not considered institutional data.

Offsite location is defined as a location where backup media can be stored that is not in the same building as the computer servers and where other systems being backed up reside.

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-03, 16 Nov 04, first draft of policy.
2. Policy reviewed on February 24, 2011.
5. Policy scope edited, expanded to include Health Sciences, July 31, 2014.