Scope

This policy applies to all IUSO owned computers, portable devices, and servers, and all members of IUSO’s workforce who have access to IUSO computers or servers.

Policy Statement

All data managed by the IU School of Optometry is considered “critical” data per university data classification guidelines regardless of whether it is clinical, research, education or administrative data. Accordingly the following safeguards shall be taken to ensure the security of all data maintained by IUSO’s systems, servers, and computers

1. All IUSO servers must be scanned every thirty (30) days and the scanning reports retained by the IT department for twelve (12) months for audit purposes. Any suspicious activity must be immediately noted and reported to the IU Information Security Office and the IUSO Compliance and Privacy Officer.

2. Anti-virus software must be installed on all systems and virus pattern files must be kept up-to-date, unless there is a documented operational necessity.

3. Any server (or machine with sensitive data) assigned an external IP address must have a documented operational necessity for being accessible to the public, and such access must be approved by the Dean.

4. Each Server Administrator must have an administrative-level username/passphrase set that is unique to that individual/server and is different from their standard user login.

5. Access to servers maintained by IUSO will be managed through the University Active Directory System which requires a university assigned user id and passphrase authentication. All users will be given an individual user folder and will be assigned access to group folders upon the request of the folder owner. Access will be terminated upon termination of employment, change in job function which no longer requires previous access, or graduation if a student.

6. Users will not be granted administrative rights to ‘desktop computers’ unless there is a documented operational necessity.
7. Unless there is a documented operational necessity, no sensitive data will be stored on the local hard-drives of desktop workstations, laptops, or portable hard drives.

8. All IUSO owned laptops must use full-disk encryption technology to protect locally stored data, unless there is a documented reason why full-disk encryption is not feasible.

9. All portable hard-drives must have password protection and encryption enabled. Any thumb-drives or other portable storage media which cannot be encrypted should not be used to store or transfer sensitive data.

10. All email accounts for IUSO faculty and staff will be placed on the University’s secure email structure. All email accounts for students will be placed on the University’s secure email structure by September 1, 2012.

11. Any smart-phone used to directly access Indiana University email should be password protected and have remote wiping enabled. The password protection should be set to time out after ten (10) minutes.

12. Data on all servers must be mirrored or backed up on a regular schedule and the data must be stored offsite.

13. Folders on the server which have access granted to more than ten (10) userids within IUSO shall be regularly scanned with IdentityFinder by the Administrator to detect any sensitive data.

14. Server System logs must be reviewed on a regular schedule by the server administrator to identify suspicious activity.

15. Servers shall be housed in the university data center and located behind the data center firewall.

16. At the time of disposal all data stored on local harddrives, servers and IUSO owned portable devices shall be securely deleted. Functioning harddrives shall be wiped with a dban(3pass). Non functioning drives shall be destroyed by drilling and crushing the disk.

Any exceptions to the requirements above must be documented and approved by the Chair of the Technology Committee unless otherwise noted.

---

**Reason for Policy**

The Indiana University School of Optometry is committed to conducting business in compliance with all applicable laws and regulations. IUSO has adopted this policy to ensure that all data maintained including any Protected Health Information (PHI), student information, financial information, or administrative information in IUSO’s control is maintained in a secure technological environment.

---

**Definitions**

**Smartphones** – A **smartphone** is a mobile phone built on a **mobile computing** platform, with more advanced computing ability and connectivity than a **feature phone**.
**Workforce** – includes all employees, volunteers, trainees, and other persons whose conduct is under the direct control of IUSO, whether or not they are paid by IUSO.

**Data** – Computer files and computer communications (e.g. email). If you can copy, paste, or edit something on a computer, it is data. A list of the University’s Data Classifications is available at http://protect.iu.edu/cybersecurity/data/classifications

**Remote Wiping** – Remote wiping is a feature integrated into most smart phone operating systems and phone/data service providers, including Android, iPhone, and Blackberry via ATT, T-Mobile, Sprint, and Verizon. Remote wiping allows a user to remotely wipe clean all data from their phone by simply calling their service provider. The service provider will then issue a command to the phone to delete all data stored on the device remotely.