IUPUI Science

Policy on the Security of Critical & Limited Access/Restricted Data and Policy on Device Security

(Originally approved May 31, 2012) (Updated 8/25/2017)

Reason for this policy

Students and patients trust us with important confidential information concerning their education and health care. Faculty and staff in the School of Science frequently handle files and data sets that include such information. State and Federal laws regulate the control of this confidential information. Misuse, loss, or release of Critical and Limited Access/Restricted Data can result in fines, criminal charges and expenses levied against the school or individuals and can adversely affect the reputation of the individuals involved, the School of Science, IUPUI and Indiana University.

Definition of confidential information

Critical and Limited access/Restricted Data is defined by 3 statutes.

1. Indiana State Law: Information is classified as **critical** if inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy or unauthorized access by an individual. The types of data include, but are not limited to, names, addresses, social security numbers, bank account and credit card numbers.
2. Health Insurance Portability and Accountability Act (HIPPA): **critical** data includes patient health data involved in treatment or research.
3. Family Education Rights and Privacy Act (FERPA): Regulates student names, contact information, grades, and courses of study, etc. Data involving grades and test scores are classified as **Limited access/restricted**.

Indiana University definitions of sensitive/ **Critical** / **Restricted** data:

- https://kb.iu.edu/d/augs
- https://datamgmt.iu.edu/types-of-data/classifications.php

School of Science Policy on the handling of Critical or Limited/ Restricted use data

Servers: Faculty or Staff storing **Critical** **or** **Limited/ Restricted use** data on School Servers must notify School of Science IT Staff so they can ensure data is stored securely.

Office Computers: Office computers must have passwords and users must log off after use. **Critical** and **Limited access/restricted** data should not be stored on local computers when possible. Files containing **Critical** **or** **Limited/ Restricted use** data should be encrypted and password protected with a strong password. It is straightforward to encrypt Office files (e.g. see http://office.microsoft.com/en-us/wordhelp/protect-your-document-workbook-or-presentation-with-passwords-permission-and-otherrestrictions-HA010354324.aspx). Entire computers should be encrypted using a strong password.

Laboratory Computers: **Critical** and **Limited access/restricted** data should not be stored on lab computers when possible. If a lab computer contains sensitive data, the computer must be password protected and files containing **Critical** **or** **Limited/Restricted use** data should be encrypted and password protected with a strong password. Entire computers should be encrypted if necessary.

Laptops: Because all laptops could potentially contain **Critical** or **Limited access/restricted** either in data files or e-mail they must be encrypted using PGP whole disk encryption with a strong password or Windows Bitlocker. Apple computer users must activate the full version of encryption available in the latest operating system versions using a strong password. Unattended laptops should be set so that the encryption is active. Similarly, if a laptop or similar device is set to sleep when the lid is closed, it should also be set to encrypt with password protection.

Mobile Devices including PDAs, iPads, smartphones: Any mobile device used to access IU e-mail or other University data, regardless of who owns the device, is required to be in compliance with IU IT policy 12.1. It must have a 4 character password with at least 2 unique characters. It should be set to auto lock after 15 minutes and lock after failed password attempts. Encryption should be used if available. If it is used to access **Critical** or **Limited access/restricted** data, it must be encrypted. If encryption is not available then the device should not be used to access or store this type of data.

Back up hard drives: Any device containing **Critical** **or** **Limited/ Restricted use** data should be encrypted. If encryption is not available then the device should not be used to access or store this type of data.

Faculty, staff and student personal and home computers. Faculty, Staff and students are required to ensure that they comply with University policies when accessing University Data using personal devices. Due to the inability to control access to personally owned computers, **Critical** **or** **Limited/ Restricted use** data shall not be stored on these devices. In cases where there is no alternative, whole disk encryption must be used.

Removable USB/flash/disk drives/cards/media: Due to the relative ease with which these devices can be lost or stolen, **Critical** **or** **Limited/ Restricted use** data shall not be stored on these devices unless they are encrypted.

Box/cloud-based file storage: **Critical** data shall not be stored on these services. **Limited/ Restricted use data can** be stored in box.iu.edu accounts in special "Box Entrusted Data Account" or "Box Health Data Account" according to the restrictions listed in the knowledge base article: https://kb.iu.edu/d/bbvn.

HELP:

If faculty or staff need clarification or help with any of these procedures, they should contact the School IT staff at soshelp@iupui.edu

University regulations: Indiana University Policy IT-02, *Policy on Sanctions for Misuse or Abuse of Indiana University Technology Resources*.

https://policies.iu.edu/policies/it-02-misuse-abuse-it-resources/index.html