

HANDLING SENSITIVE DATA

What exactly is critical information?

Indiana University outlines critical information at the following Protect IU page:

<https://datamgmt.iu.edu/types-of-data/data-guide/index.php>

General Concepts

Indiana University has outlined some general concepts when handling sensitive data:

- Keep what you view on your computer screen private.
- Keep your equipment safe.
- Keep security in mind whenever you work off campus.
- Find out what backup solutions your department recommends, and keep data backed up.

<https://protect.iu.edu/online-safety/protect-data/sensitive-data/index.html>

Guidelines for handling electronic institutional and personal information

Click the following link for some general guidelines to handling electronic data:

<https://protect.iu.edu/online-safety/protect-data/sensitive-data/guidelines.html>

Sharing Sensitive Data

Two methods of sharing are:

- **Slashtmp**
 - *At Indiana University, the Slashtmp service provides graduate students, faculty, and staff a way to share data with others via a web interface. It is particularly useful for sharing files that are too large to send via email. Slashtmp has two versions:*

***Simple:** Use the Simple version if you're transferring non-sensitive research data.*

***Critical:** You must use the Critical version if you're transferring data that's subject to HIPAA regulations, or other information classified as critical at IU (e.g., Social Security numbers, credit card numbers, or bank account numbers).*

From: <https://kb.iu.edu/d/angt>

- **Cisco Registered Envelope Service (CRES)**
 - CRES is a way to encrypt e-mail messages. At Indiana University, do not send sensitive data via email unless:
 - ***It is required by your role within the university.***
 - ***The message either:***
 - is encrypted by the Cisco Registered Envelope Service (CRES), or
 - stays within the IU email systems (Exchange; not Imail or Umail).

Should I send confidential information via e-mail?: <https://kb.iu.edu/d/aktv>

Ensuring mail sent is encrypted by CRES: <https://kb.iu.edu/d/bbum>

Secure Data Removal

Data must be securely removed from the media (hard drives, USB flash drives, floppy disks, CDs, memory, etc) once the data or the device is no longer needed or active. This page outlines the measures to take:

<https://protect.iu.edu/online-safety/protect-data/data-removal.html>