Indiana University’s policy on the security of IU data, scan for sensitive data, and mobile device security.

The security of IU data is your responsibility!

The safe storage and security of sensitive university data is your responsibility. Of particular importance are critical, restricted and university internal data, which the university groups under the label of sensitive data. Sensitive data is often protected by Indiana or federal law as well as by university policy. Violation of these statutes can result in civil and criminal penalties for both you and the university. Violating university policies can lead to sanctions for individual employees, up to and including termination of university employment.

For a clear explanation of the various types of sensitive data, please read the Knowledge Base article and references within “What is sensitive data, and how it is protected by law?”

Some key points and additional references:

- Do not store data that is not required, and delete data when it is not any longer needed.
- Do not store sensitive data on insecure devices such as thumb drives, CDs, or other easily lost and removable media.
- Do not save/store any SSNs unless absolutely required by law. Contact UITS-NW for options. If you must collect a SSN, delete it from the source as soon as you enter it into a university central system.
- For mobile devices (smart phones and tablets) that access university email or other university data please read the requirements section on IU Mobile Device Security below.
- University laptops that are used to access or store university data must be encrypted.
- To dispose of devices (equipment and/or media) that contain university data, call the UITS-NW Support Center.
- Know and understand the Family Educational Rights and Privacy Act (FERPA) law. If you have not already done so, please complete the 10-15 minute online tutorial at FERPA.IU.EDU to gain a basic understanding of the law and your responsibilities.
- Please contact the UITS-NW Support Center to discuss appropriate storage options for critical data.

IU Mobile Device Security

This is a reminder of Indiana University’s Mobile Device Security Standards, otherwise known as Policy IT-12.1. In summary, the policy states that all IU employees (faculty, staff, affiliates and student-workers) who use a mobile device, regardless of who owns the device, to access, store or manipulate institutional data, including accessing their IU email, must meet the following requirements on the mobile device:
- Require a minimum 4-character passcode using at least two unique characters
- Require your device to auto lock after a maximum of 15 minutes of inactivity
- Require your device to lockout or wipe after 10 incorrect access attempts

**Mobile devices should never be used to access, store, or manipulate critical information.**

Employees are required to **immediately** report lost, stolen, or otherwise compromised devices to the University Information Policy Office (UIPO) at it-incident@iu.edu. Additionally, the device must be wiped before transferring ownership (sales, trade-in, etc.).

You can view policy IT-12.1 in its entirety at POLICY.IU.EDU and selecting Information and IT.

---

**Notice of Secure Scan for Sensitive Data**

As recommended by the University Information Security Office (UISO), UITS Northwest performs periodic scans of campus computing resources to reveal the location of any potentially sensitive information. A few common examples of sensitive or critical data are:

- Social Security Numbers (SSN)
- Credit Card Numbers
- Bank Account Numbers
- Driver’s License Numbers
- Protected Health Information
- Passwords

University policy, in accordance with State law, requires removal of sensitive data if it is not absolutely necessary or to take appropriate steps to protect the information. For example, to protect sensitive data, the University mandates the use of UID numbers in place of social security numbers, in most instances.

An example of necessary use of Social Security Numbers would be where a government agency requires the information. In this case, the data needs to be safeguarded with encryption technology. However, use of SSNs in documents such as class rosters or employee records (where the information can be retrieved from University central systems) are examples of data which is NOT required, and the SSNs need to be removed. Removal of the data can be done by redacting all but the last four digits of the number, deleting sensitive data from the document, or deleting the entire document.

If you have any questions about this process, or the methods for safeguarding sensitive data, please contact the UITS Northwest Support Center so that we may help assure that we are acting as good data stewards as well as complying with appropriate State and Federal regulations. The goal is to have no unnecessary sensitive data in electronic storage in any location: file server, local hard drives, or portable media.

You can get more information on IU’s classification levels of institutional data by visiting DATAMANAGEMENT.IU.EDU and selecting review data classifications.

---

**University policies and data security information**
It is your responsibility to know and understand University policies regarding handing of university data. For more in-depth information on university policies and other data security information, please search the list of resources below at the following web sites:

- **KB.IU.EDU**
  - What is sensitive data, and how is it protected by law?

- **DATAMANAGEMENT.IU.EDU**
  - Classifications of Institutional Data

- **FERPA.IU.EDU**
  - Student Privacy & FERPA Overview and Tutorials

- **POLICY.IU.EDU**
  - IU Privacy of Electronic Information and Information Technology Resources (IT-07)
  - Security of Information Technology Resources (IT-12)
  - IU Cyber Risk Mitigation Responsibilities (IT28)

- **PROTECT.IU.EDU**
  - Protecting Red-Hot Data
  - Best Practices for Handling Electronic Institutional and Personal Information

**We are your connection to IT@IU!**

Thank you for your attention to keeping sensitive University data secure and, whenever a question arises, please do not hesitate to contact the UITS-NW Support Center for guidance and assistance.

**UIITS Northwest**
Hawthorn 108
iunhelp@iun.edu
http://www.iun.edu/technology
219-981-4357 (HELP)

You may notice this message has links, but it has been digitally signed. Feel free to verify our certificate before clicking any links.