STORING SENSITIVE DATA

**BEST**: Do not store unless absolutely necessary

**ACCEPTABLE**: (Non-critical only!) IU Box ([box.iu.edu](box.iu.edu)), JSoM File Server (AKA Faust)

**UNACCEPTABLE**: USB Drive, computer desktop/hard drive, all laptops (business and personal), phone, and public cloud storage such as Dropbox or SurveyMonkey

SENDING SENSITIVE DATA

**BEST**: Share data from where it is being stored without making a new copy (e.g., share from IU Box)

**GOOD**: Slashtmp ([slashtmp.iu.edu](slashtmp.iu.edu))

**GOOD**: Encrypted email—How? [https://kb.iu.edu/d/bctk](https://kb.iu.edu/d/bctk)

**ACCEPTABLE**: (Non-critical only!) IU Exchange email with “Confidential” in the subject

**UNACCEPTABLE**: non-IU email, web server, USB drive, unsecured paper copies, and social media

INDIANA UNIVERSITY SENSITIVE DATA CLASSIFICATIONS

CRITICAL DATA

Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals.

- Social Security number
- Drivers License number
- Passport and Visa numbers
- State ID number
- Certification/license numbers
- All payment card numbers
- Student loan information/numbers/credit
- Student academic transcript
- Student ethnicity, birth country, citizenship
- Donor/foundation information
- Health information
- Passwords and passphrases
- PIN numbers
- Security and access codes

REstricted DATA

Because of legal, ethical, or other constraints, restricted data may not be accessed without specific authorization, or only selective access may be granted.

- Date of Birth/Age
- Gender
- Emergency contact
- Home mailing address/phone
- Ethnicity
- Military/veteran status
- Citizenship/visa status
- Country of Birth
- Work Authorization (I-9)
- Job action reason (termination or leave)
- Benefits enrollment information
- Payroll information
- Marital status

UNIVERSITY INTERNAL DATA

This data may be accessed by eligible agents of the university in the conduct of university business; access restrictions should be applied accordingly.

- IU ID Number
- Preferred name
- Prior name
- Position information
- Part time/full time indicator

Learn more about Indiana University Data Classification Categories: [datamgmt.iu.edu/classifications.shtml](datamgmt.iu.edu/classifications.shtml)

Unsure what to do? Send an email to musicits@indiana.edu
HOW TO SECURE YOUR DEVICES

KEEP YOUR DEVICES UPDATED TO STAY SECURE

MOBILE PHONE

Do you access IU email or other systems from a smart phone?
Secure it by requiring a passcode lock and enable automatic screen lock after a short period of inactivity.

TABLET

Do you use an iPad or tablet for work?
Secure it by requiring a passcode lock and enable automatic screen lock after a short period of inactivity.

LAPTOP

Do you use a laptop for work?
Do not store critical data on the hard drive. Require a password to unlock. All IU-owned laptops must be encrypted—contact IT staff.

DESKTOP

Do you use a desktop at home to access the IU network?
Do not store sensitive information on the hard drive. Set a password on the login screen. Make sure you run an anti-virus program. Do not store your IU passphrase on the hard drive or allow browser applications to store it.

PERSONAL

Do you use your personally owned mobile device to access IU systems?
Do not store critical data on the hard drive. If you access IU systems on your device, secure it by requiring a passcode lock and enable automatic screen lock after a short period of inactivity. (IU policy 12.1)

SYNC

Do you sync devices?
Be mindful of applications that sync to multiple devices. Make sure ALL devices are secured.

Unsure what to do? Send an email to musicits@indiana.edu