Email Best Practices

At Indiana University, employees must not send critical data via email. Restricted data may be sent by email only if:

- It is required by your role within the university.
- The message is encrypted (e.g. use of IU email server, CRES, Slashtmp) For more info: [Should I send confidential information via email?]

Critical Data

If you have approval to share **critical** student data in the course of your business operations (SSN, credit card information, etc…):

1. Ensure the recipient is a school official with a legitimate need for the information

2. Utilize the critical version of slashtmp to attach a file as this will **encrypt** and allow you to send up to 4 GB of data. For more information: What is slashtmp and how do I use it?

Restricted Data

Email sent from one account on a central IU email server (Exchange or Cyrus) to another IU email account on these servers has technical and physical safeguards, and is considered secure. Do not send messages to an alternate email such as imail, umail, gmail, etc… Use of Microsoft Outlook on your office systems configured by your LSP or remote desktop to access your IU email ac-count from home are both acceptable methods for accessing and sending email securely to other IU employees.

When sending **confidential** restricted data (e.g., such as name, DOB, ID#, ethnic data, financial aid status, sensitive personal information about the student's health or family etc...), use the Cisco Registered Envelope System (CRES) which **encrypts** the data in the event that the message leaves the IU network. You invoke CRES by including **Secure Message** or **Confidential** in the Subject line. For more info: What is the Cisco Registered Envelope Service (CRES)?

When in doubt whether the email content is confidential or whether the restricted data will be forwarded outside of the IU network, please use CRES!

Phishing

Phishing is a form of email fraud where scammers use email messages that appear to come from a legitimate company or institution, such as your bank or university, and they ask you to "update" or "verify" your personal information. Do not provide your social security number or confidential personal information in response to an email request. For more info see: What are phishing scams and how can I avoid them?

*For questions regarding system tools contact your Local Service Provider.

What is sensitive data at Indiana University?

The following data elements require the highest level of protection. Please note, this is not a comprehensive list, but can be used as a guide for identifying data assigned the restricted and critical data classifications.

FEDERAL AND STATE LAWS
Data that is regulated by Federal or State laws including but not limited to:

◊ Family Rights and Privacy Act (FERPA)
◊ Health Insurance Portability and Accountability Act (HIPAA)
◊ Electronic Communications Privacy Act (ECPA)
◊ Payment Card Industry Data Security Standard
◊ Gramm-Leach-Bliley Act (GLBA)
◊ Freedom of Information Action (FOIA)
◊ Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation)
◊ Indiana State Data Protection and Security Laws Ind. Code 4-1-10, 4-1-11, 24-4-14

RESTRICTED DATA

Individual Student University Records

·Grades/Transcripts*
·Courses taken/Schedule
·Advising records
·Educational services received
·Disciplinary actions
·Student Financial Aid, Grants, and Loans
·Financial account and payment information
·Admissions information including test scores, high school GPA, class rank
·Personal Information such as:
Date of birth, gender, marital status, ethnicity, country of citizenship, visa information, immunization, residency, veteran status, military status, student affiliations, parent information, emergency contact information
·Student directory information restricted by student request (FERPA restrictions)

When restricted data is breached, student notice is required.

***Official Transcripts treated as critical data**

CRITICAL DATA

SSN and Other Personally Identifiable Information:

Name (First name or initial and Last name), when stored or displayed with one or more of these data elements:

- Social Security Number
- Driver's license number
- State identification card number
- Financial account numbers such as credit, debit, or bank account numbers
- System Password/PINs
- Identifiable health information

Requires notice to the Indiana Attorney General within 2 business days if information is breached without the necessary encryption. In addition, notification to the student is required. If you suspect data has been breached, contact it-incident@iu.edu.

INQUIRIES?

Contact your Department's IT Security representative to inquire about the security measures that must be implemented for all data that is not considered public. You may also contact the Committee of Data Stewards at iudata@iu.edu with questions about data classification.

For more information regarding data classification: http://datamgmt.iu.edu/classifications.shtml