Sensitive Data Policies and Email Encryption

What is *Sensitive Data*?

In general, sensitive data is information that can be damaging and/or violate privacy laws if it falls into the wrong hands. However, at IU the term *sensitive data* (or *sensitive institutional data*) has a specific and well-defined meaning. Furthermore, there are different classifications of sensitive institutional data as defined in the Classifications of Institutional Data document. These include:

1. **Critical** - This is the most sensitive classification and includes things like HIPAA-regulated medical data, student records like transcripts, banking information, social security numbers, and passport/visa numbers
2. **Restricted** - This includes things like demographic information (age, gender, ethnicity, etc) and payroll information.
3. **University-internal** - The most common piece of university-internal data is a person's University ID number but this classification also includes other IU internal things like position information and employment status
4. **Public** - Information in this category is not restricted and includes publicly accessible information like names, titles, and compensation.

This is in no way intended to be a complete listing of all the sensitive data types. Rather, it is just a summary to give you a feel for the different classes of sensitive data. You should read and familiarize yourself with this Data Storage and Handling tool. Note that you can select the type of data, and the tool will tell you the classification and the approved, secure handling instructions.

Account and Mobile Device Security

Please see the KB page SICE Account Security Recommendations for information about securing your IU accounts and mobile devices so you are in compliance with IU security policies.

Email Background

When you send an email, it typically goes across the network and is stored in what is called "clear text". What that means is that anyone with access to the network connection or files on the email server can read the email message. Encryption can be used to "scramble" the message so it cannot be read without a password. So, if sensitive information is sent using email, care must be taken to ensure that email leaving the IU mail system is encrypted. This page describes the mechanisms you can use to ensure the secure transmission of sensitive data via email so you are in compliance with IU security policies.

Sensitive Data and Email

> **Critical Data**
>
> In most cases, you will want to avoid sending ***critical*** sensitive data via email if at all possible. This section applies only to non-critical sensitive data in the restricted and university-internal classifications (see previous section). If you have a need to send critical data via email, please cont act the IT staff so we can discuss options and appropriate safeguards.

Special care must be taken when sending any sensitive data via email. First of all, if you can avoid sending sensitive data via email that is preferable. However, for many of us sending sensitive data via email is part of your job and hard to avoid. So, here are two options for sending *non-critical* sensitive data.

Option 1: CRES Service

IU has a CRES (Cisco Registered Envelope Service) encryption service that is extremely simple to use. All you have to do is put "[Secure Message]" (including the square brackets but not the double quotes) in the subject of the message and that's it. It doesn't get much easier than that! The way this works is as follows:

- If the message stays within the IU email system, it will not be encrypted.
- If the messages leaves the IU email system, it will be encrypted. So, if the message is sent or forwarded to a non-IU email address it will be automatically encrypted and the recipient will receive notification with instructions on how they can read the original message.

So, if you need to email non-critical sensitive data (including a 9-digit IU ID number) just put "[Secure Message]" (including the square brackets but not the double quotes) in the subject of the email and you are in compliance with IU email policy. Do note, however, that this requires that you be using the IU mail servers for your outgoing email. This will be true for most people using the IU mail system but if you are using a non-IU email system and have questions on how you can take advantage of this service, please contact the IT staff.

Option 2: Manual Encryption

You can also manually encrypt email messages you send which means they will be encrypted even if they stay within the IU mail system. This is a more secure method but setting it up is more involved. Furthermore, it takes a bit of coordination between the sender and receiver since both must have encryption keys set up and they must be made available to each other. So, if you rarely send sensitive email you will almost certainly just want to use the CRES service. However, if you frequently send sensitive emails to a small group of people it is probably worth setting up manual encryption.

To set this up, there are 2 parts. First, you and the people you will be sending email to must create your encryption keys (aka. a *client certificate*). This can be done as follows:

1. Create a S/MIME certificate per: Using S/MIME client certificates at IU
2. Import the certificate into your mail program:
    a. Windows/Outlook: Using S/MIME Client Certificates with Microsoft Outlook for Windows
    b. Mac/Apple Mail or Outlook: Using S/MIME Client Certificates with Apple Mail and Outlook for OS X
    c. Thunderbird: Using S/MIME Client Certificates with Thunderbird

Once that is done, just click Encrypt (Outlook) or Security>Encrypt This Message (Thunderbird) when sending any email containing sensitive information (see links in step 2 above for details) and your message will be encrypted. Most other modern mail programs also incorporate this feature. Keep in mind that encrypting email relies on you having access to the recipients public encryption certificate. If you are using the IU ADS GAL (as noted above) you will have access to anyone at IU who has created and published their public certificate. For anyone else, you will need to manually exchange public keys.

Further Reading

This KB page is intended to be a simple summary of a rather complex issue involving various IU policies. Below are various reference documents if you want to pursue this subject further.

- SoIC Storage Services and Sensitive Data
- Mobile Device Security Standards
- What is sensitive data, and how is it protected by law?
- Classifications of Institutional Data
- Should I send confidential information via email?
- Student use of email for work-related purposes
- Secure File Transfer Alternatives
- Data Management at IU and the Critical Data Guide
- What is the Cisco Registered Envelope Service (CRES)?
- How can I ensure that mail sent from my Exchange or Cyrus account to an outside address is encrypted by CRES?
- IT-21: Use of Electronic Mail