**Sensitive Data FAQs**

**What is Sensitive Information?**

The University defines sensitive information as “information of a confidential or proprietary nature and other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements, or University policy.” (*Source:* [*Information Security Office (ISO*](http://security.louisville.edu)*) website glossary of security terms*).

**How do I determine if my area deals with sensitive information and where it resides?**

A survey of your user community can help to identify the use of sensitive information. This can be done by discussion or by an electronic survey using Excel or other application. It is important to capture information regarding the data type, medium, owner and location. Consider current and historical information from its creation to its destruction in both hardcopy and electronic format.

**Where can I find guidelines on how to handle or store sensitive information?**

Handling guidelines (storage, transmission, disposal, labeling) can be found on the Information Security Office’s (ISO) website: <http://louisville.edu/security/files/ClassificationandHandlingGuide.pdf> . Additional information is provided within the University policies and standards and available on the ISO website at: <http://louisville.edu/security/policies/iso-policies> .

**What is encryption?**

A process used to secure data so that only authorized users can access or read the information.

**Why should I use encryption?**

Encryption meets regulatory requirements for the securing of sensitive information and therefore, is required for all devices (University or personally owned) that store, process or maintain University sensitive information. Additional information regarding encryption can be found on the ISO website: <http://louisville.edu/security/resources/faqs/encryption-faqs>

**Where can I find information on encryption software and how to encrypt my desktop or laptop?**

Documentation regarding free University encryption software can be found on the IT websites at: <http://louisville.edu/it/departments/enterprise-security/information/pgp-encryption-information> or

<https://itechxpress.louisville.edu/softwareresales/free/encryption/>. IT currently encourages MAC users to utilize the built in encryption native to the device. Be aware that unlike the Enterprise managed Symantec solution; IT does not centrally manage native MAC encryption and is therefore unable to assist in the recovery of a forgotten password.

**How can I tell if my device is encrypted?**

Encryption verification can vary by device and product. Therefore it is best to check with your Tier I or the device manufacture. Examples of current University utilized encryption can be found on the ISO website at: http:// louisville.edu/security/resources/how-to

**Do I need to encrypt my smartphone or mobile device such as a flash drive? How can I do this?**

Encryption is required if you receive University sensitive email or calendar information on your smartphone or if you store this information on external devices such as a flash drive or tablet. Flash drives can be purchased encrypted or MAC users can utilize the MAC native encryption tool to manually encrypt a flash drive. A MAC encrypted flash drive cannot be read on a PC. Smartphone encryption features require the activation of the passcode or encryption setting. Additional information on securing mobile devices can be found on the manufacture’s website or on the ISO website at:

http:// louisville.edu/security/resources/how-to

**When do I need to encrypt an email message? Where can I find information on email encryption?** Per ISO Policy PS018, encryption of University sensitive information maintained on or transmitted by computing devices is mandatory.  Encryption of sensitive information reduces the risk of unauthorized access and increases the University's ability to maintain regulatory compliance, contractual obligations and the expectations of our constituents and the community at large.  The University provides a secure email solution for sending sensitive information from the louisville.edu exchange system (@exchange.louisville.edu) to external parties. Email sent from one @exchange.louisville.edu account to another @exchange.louisville.edu account is secure; however, email sent to student CardMail accounts, employee preferred accounts or any external account must utilize the secure email feature [SEND SECURE]. Additional information on securing email can be found at: <http://louisville.edu/email/cisco-secured-email/sending-a-secured-email.html> or <http://louisville.edu/email/cisco-secured-email> .

**Is there a shortcut or easy way to ensure the use of the email encryption [SEND SECURE] feature?**

Enterprise IT is currently exploring an add-in option for Outlook. In the meantime, a quick step button can be created to reduce the potential for error and the time required to ensure your email is sent securely. Directions on how to create a quick step can be found on the ISO website at: <http://louisville.edu/security/resources/how-to>

**What is Secure FTP?**

File Transfer Protocol (FTP) is a network protocol that manages file transfers between computers. Secure FTP encrypts commands and data, preventing sensitive information from being transmitted in clear text over a network.

**How do I use Secure FTP?**

Various software programs can be used to process Secure FTP. It is suggested that you work with your Tier I for technology related hardware or services. Free software such as Secure Shell SSH Client and WSFTP Client is available from the IT iTech Xpress website at: <https://itechxpress.louisville.edu/softwareresales/customer/free.php?free_cat=5>

**How do I obtain hard drive erasure software?**

It is suggested that you work with your Tier I for technology related hardware or services. A free copy of erasure software can be downloaded from the IT iTech Xpress website at: <https://itechxpress.louisville.edu/softwareresales/customer/free.php?free_cat=5>

**How do I arrange for Shred-It services?**

Contact the University’s Purchasing department for questions regarding the use of Shred-It services.

**What about printers and multifunctional devices?**

Xerox multifunctional devices purchased through the University’s Copy Management Program are equipped with security features such as encryption and nightly overwrite. Additional device information can be found on the ISO website at <http://louisville.edu/security/resources/tools-and-tips>

**What efforts are underway to address sensitive data handling?**

Information Security education is currently provided as part of the New Employee Orientation, UBM/UBT, HIPAA and PCI training modules and departmentally as requested. A working group representing areas across the University has been created to address the protection of sensitive data. Steps are currently underway by Enterprise IT to further secure data within specific enterprise systems and HR is reviewing processes in order to reduce or eliminate the need to retain or process some forms of sensitive information.

**For technical assistance contact your Tier I or the IT helpdesk at 852-7997.**