

**The information in this word document was extracted from this UofL Website:**

<http://security.louisville.edu/PolStds/ISO/PS012.htm>

**Please visit that website for more details!**

**What is considered sensitive information that would require your machine or device (laptop, jump or flash drive, external drive) to need encryption?**

### **Sensitive Information**

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. This includes (but is not limited to) identifiable medical and health records, grades and other enrollment information, credit card, bank account and other personal financial information, social security numbers, grant reviews, dates of birth (when combined with name, address and/or phone numbers), user IDs when combined with a password, etc.

**Note:** Sensitive information does not include personal information of a particular individual which that individual elects to reveal (such as via opt-in or opt-out mechanisms).

**What recommendations do my Tier 1 staff (at Kent School – Debra Evans, Dennie Carter, and Shelly Geraghty) have for me if I work with information that is of a sensitive nature?**

- Familiarize yourself with the definition of sensitive data. Ask one of us if you have questions in regards to whether your data is sensitive.
- Store your sensitive data on the IT networked H: drive – this is secure and backed up nightly, and only you can get to your H: drive with your userid and password. Cost is minimal.
- If you use an external or flashdrive to transport or sensitive data, purchase one that comes with encryption software already on it. Check with one of us for our recommendations. Those who work with grants – check with Sally Atcheson on which flashdrive to purchase.
- Have your Tier 1 install Guardian Edge encryption full disk software if your computer warrants the installation.
- Visit the ISO website to familiarize yourself with policies. Ask if you have questions – call Matthew Witten directly if you are not sure about your data. His userid and phone number are in the GroupWise addressbook.

**What about information I send over my email account?**

### **University Secure and Encrypted E-Mail**

The University uses "Post X" e-mail encryption to allow for secure sending and receipt of e-mail.

More information on this tool including how to configure and use it is located at the following web site: <http://louisville.edu/it/services/e-mail/encryption.html>

---

## **What are the workstation policies for UofL?**

### **POLICY:**

All workstations and other computing devices shall:

- be maintained in an environment and manner so that access is reasonably restricted to authorized users only;
- be used in a prudent manner so that data, system and network integrity is maintained to the highest degree reasonably possible; and
- have operating systems and other software maintained in the most up-to-date and secure manner reasonably possible.

### **Technical and physical standards:**

- **System Maintenance:**
  - All computing device operating systems and other software should be kept up-to-date by reviewing security updates, patches and tools on a regular schedule but not less often than every 90 days. Automated update capabilities must be turned on.
- **Physical System Access:**
  - Reasonable efforts should be made to limit and/or monitor physical access to computing devices to only authorized personnel. The computing device display screen should be positioned to minimize the chance for viewing by unauthorized individuals, where appropriate and feasible.
- **Systems used to store, transmit or access electronic Protected Health Information (ePHI).**

In addition to the physical security requirements above, each responsible area must:

  - Implement and maintain physical safeguards to restrict access to only authorized users for all computing devices that store, transmit or access ePHI.
  - Define the allowable functions, how these functions are to be performed and required physical surroundings of computing devices that access ePHI.
- **Software:**

- Operating systems and software currently supported by University IT should be used for University computing. See [Supported Software List](#) for more information.
- Other operating systems and software are allowed if such software is:
  - currently supported by the vendor with security updates provided and applied as applicable;
  - approved for the use by and supported by your School/Division's technology management; and
  - in compliance with [IS PS004 Policy Exception Management Process](#).  
**Note:** This is an example of the type of exception that will generally require only proper completion of the initial form and not the "Policy Exception Management Template".
- **Logical System Access and Security:**
  - **Passwords**

All computing devices should require entry of a user ID and complex password. See [IS PS007 User Accounts and Acceptable Use](#) and [IS PS008 Passwords](#).
  - **Administrator or Administrative Accounts**

The Tier 1 support staff for the School or Division should be used for installation of any software or performance of administrative functions on computing devices. If the Tier 1 staff is not routinely used, the School or Division should have a policy and procedure for permitting other individuals to engage in these tasks.