Information Security – User Awareness

Information Security Definition: to ensure the confidentiality, integrity and availability (CIA) of information and information systems by protecting against unauthorized access, modification or disclosure (i.e., the right people see the right information at the right time).

Information Security Office: Who are we? Information Security is not part of IT but rather under the Audit and Compliance Office. We work closely with IT and with the Privacy (HIPAA) and Controllers (PCI) Offices. Our services are free**.**

Goal: Provide policies, awareness and assistance for users in order to protect University assets (hardware/software, data, and personnel). Provide procedures and recommendations to ensure compliance, eliminate the potential for an incident and lessen audit findings.

Focus Areas:

Data – all data, specifically "sensitive" data. Regulations: HIPAA, FERPA, PCI, Export Controls, HB5 (includes paper or electronic)
Hardware/Software – University and personal desktops, laptops, mobile devices, University servers and applications

Awareness:

Orientation and University training sessions
Departmental Supplements/Training (HIPAA, HSC Campus, etc.)
UofL Today Articles
Website -- http://louisville.edu/security
On-site training sessions or security assessments

Responsibility: **Information Security is the responsibility of EVERY user.**

- Never share or post your user password and keep security codes, keys, equipment, etc. secure
- Know your data, its classifications and any regulations – handle accordingly
- Immediately notify your supervisor or the Security Office if you suspect an incident
- Email –encrypt "sensitive" data when sending outside of the University system [SEND SECURE]
- Email – never open attachments or click on links from unknown/unexpected senders
- Never share or store 'sensitive' data with external parties without appropriate agreements
- Mobile Devices (laptops, flash drives, CDs, tablets, smart phones) – must be encrypted if storing 'sensitive 'data
- Ensure all computing devices are updated with approved anti-virus software and patches
- Familiarize yourself with the University Information Security Policies located at: http://louisville.edu/security/policies

University of Louisville Definition of 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) full name or first initial and last name and employee ID (**in combination**), 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. 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) (see Information Management and Classification Standard)

Contact the Information Security Office if you have questions, need training or suspect an information security incident.

Kim Adams 852-6692 or Lisa Cooper 852-0567
Security Email: isopol@louisville.edu
Compliance Hotline: 877-852-1167

Information Security User Awareness

Password Guidelines:	
Do:	**Don't:**
➢ Always use at least an 8 character password with a combination of upper/lower case, alphabets, numbers and special characters (*, %, @, !, #, $) ➢ Use a password you can remember ➢ Change your password per the policy or immediately if it has been compromised	➢ Share your password with others, even your manager or IT ➢ Post your password where others can find it ➢ Use the same password for business and personal accounts
Email/Internet Guidelines	
Do:	**Don't:**
➢ Use for University business purposes ➢ Follow Email Storage (Archive) guidelines ➢ Contact the help desk about suspected spam or virus messages ➢ Send sensitive messages securely ➢ Abide by the Internet Use Policy	➢ Open unexpected or unknown emails ➢ Send unsolicited mail messages ➢ Use University mail in a manner that degrades or interferes with the job ➢ Use internet to view, store or transmit obscene or pornographic material ➢ Use the internet to download copyrighted material
Sensitive Data Guidelines	
Do:	**Don't:**
➢ Understand the type of data you work with and any federal, state or industry regulations ➢ Transmit securely, label appropriately, use only encrypted flash drives, shred before disposal, store securely	➢ Send or store sensitive data publicly without encrypting (includes texting, cloud storage, external email) ➢ Store, share or transmit data without authorization – Business Associate Agreement may be required for PHI ➢ Leave sensitive material in plain site

Additional information regarding University of Louisville's Information Security Program can be found at: http://security.louisville.edu. For questions, please contact the UofL Information Security Office at: isopol@louisville.edu or Kim Adams: 502.852.6692 or Lisa Cooper 852-0567.