UNIVERSITY OF LOUISVILLE.

InfoSec

Service Account Email Address: isopol@louisville.edu
Website: http://louisville.edu/security

Information Security Office

Newsletter II: Information Asset Management and Classification

Audience: All Faculty and Staff who are involved in handling sensitive data as part of their job function.

Background:

This is the second of several information security awareness emails meant to help you evaluate the Information Security controls used in your area and to help you identify potential risks. The questions below are a sample of what would be asked during a formal risk assessment conducted by the Information Security Office. The information provided here is meant to help you initiate conversations within your unit that will result in decreased risk of information exposure.

Topic: Information Asset Management and Classification

Often we think of an asset as something tangible, like computer equipment. However, *information* assets (data) are a valuable and vital part of our daily workflow. An information asset is a body of knowledge that is organized and managed as a single entity that usually has some form of value. Examples of University information assets include student records, patient records, research data and Human Resource records. Information assets can be classified in many ways sometimes by relative importance, sensitivity or frequency of use. When considering information asset management, you should also consider the information's importance to the unit or the University and the information's classification.

Classifications at the University fall under two categories (*Sensitive, and Non-Sensitive). **Sensitive /Confidential or Proprietary-internal use only** information includes sensitive personal and or University information that would not be routinely published for unrestricted public assess or where disclosure is prohibited by laws, regulations, contractual agreements or University Policy. **Non-sensitive/public** information is information that is generally available to the public, or that, if it was to become available to the public, would have no material or adverse effect on the University.

Questions to consider when evaluating Information Asset Management and Classification include:

1. What types of information assets does the department handle as part of its daily workflow?

2. Have the information assets (electronic and hardcopy) been inventoried in your area and do you have supporting documentation to demonstrate this?

3. Are users aware of any regulations and subsequent safeguards for information they own, use or may come into contact with in their area?

4. Has the department determined classification (sensitivity) and owners of its information assets?

5. Has the department developed policies and procedures to ensure that sensitive information assets are properly secured, handled, retained or destroyed?

6. Does the department periodically review information assets to ensure their security?

7. Does the department have a documented process and procedure to handle access control when someone joins or leaves the unit?

Information Security policies regarding data classification and handling:
http://louisville.edu/security/policies/data_class

*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).

Questions: If you would like to have a copy of Newsletter I (Physical Security Controls) go to the following web site: http://louisville.edu/security/files/newsletter-i-physical-security/view. If you have follow up questions they can be directed to our email service account at isopol@louisville.edu