UNIVERSITY OF LOUISVILLE.

InfoSec

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

Newsletter I: Physical Security Controls

Introduction:

The Information Security Office will be working to raise the awareness/preparedness of the University community regarding risk assessments. This is the first of several information security awareness Newsletters meant to help you evaluate the information security controls used in your area and to help you identify potential risks. The questions listed here are a sample of what would be asked during a formal risk assessment conducted by the Information Security Office.

Topic: Physical Security

Does your department manage physical access to the sensitive data stored in the area you work in, including the devices you use to handle sensitive data? Have you considered the potential for sensitive data exposure or modification due to unauthorized access? If your answer to these questions is 'no' then you should evaluate the need to develop a physical security management plan. Listed below are questions to assist you when reviewing this topic:

1. Does your department have a secure perimeter? If applicable, are door codes/keys restricted to authorized personnel only?

2. Are computers located in areas that are not easily accessible to outsiders or away from high-traffic areas, for example instructor's offices and administrative staff? Do your faculty and staff understand their responsibility to ensure that doors and windows are closed and locked?

3. Does the department have a procedure to log physical access provided to vendors and visitors?

4. Does the department send regular awareness reminders to staff members addressing the importance of securing items such as laptops, keys, office doors, utilization of laptop and screen locks, and securing printed documents that contain sensitive data?

5. Does the department have a process for managing physical security in regards to employee turn-over for those who are terminated, transfer or retire (returned keys, changing codes, etc.)?

6. Do you have a scheduled review of physical access to prevent oversight?

7. Has all the equipment used to store sensitive data in the department been inventoried? This should include items that may not be tagged by the University's Inventory Control process for example, flash drives.

8. Does the department have media handling guidelines which include securing sensitive data, including the proper removal of data from portable devices such as CD's, diskettes, DVD, Zip disks, USB, etc. Reference the following ISO policy for additional information: http://louisville.edu/security/policies/isopolicies/iso-ps016-inventory-tracking-and-discarding-of-computing-devices

9. Do you have a procedure to validate that all portable data storage devices containing sensitive information have been properly secured and encrypted? Reference the following ISO policy for additional information: http://louisville.edu/security/policies/iso-policies/iso-ps018-encryption-of-data

10. Does the department have a process to validate security settings and encryption on removable storage devices and is this completed regularly?

11. If you are a server administrator (of a server located outside of the data center) have you developed controls for back up's, fire, water, temperature control, UPS, surge suppression and physical access to this system? Reference the following ISO policy for additional information: http://louisville.edu/security/policies/iso-policies/iso-ps013-server-computing-devices

12. Does your department have procedures to report security incidents including loss, theft or compromise? Reference the following ISO policy for additional information: http://louisville.edu/security/policies/isopolicies/iso-ps006-security-incidents

This Newsletter is the first in a series of informational guides that will be released in the upcoming weeks. The information is intended to help you begin the process necessary to identify areas that should be mitigated if necessary to reduce your department's potential information security risks. If you questions please feel free to contact the Information Security Office at isopol@louisville.edu. Thank you.

**Also, please encourage others who may find this information helpful to subscribe to our Listserv by sending us an email to isopol@louisville.edu.