Newsletter III: Departmental Information Security Policies

Introduction:

The Information Security Office is working to raise the awareness/preparedness of the University community regarding risk assessments. This is the third 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 University's Information Security Office.

Background:

Consistent Information Security policies and supporting standards provide a common approach to compliance, regulatory and operational requirements.

- The policies published by the University's Information Security Office provide a baseline or minimal requirement. Departments can, and in some cases are required to, implement more stringent policies or procedures in order to meet regulatory or contractual requirements of their specific work environment.

- Regulations such as HIPAA and PCI require that departments have their own set of documented policies and procedures for handling sensitive data.

- Policies should be reviewed regularly, updated when required and disclosed to users.

- In addition to the ISO website http://louisville.edu/security the Information Security Office's policies can also be found in the University Policy and Procedure Library, at http://louisville.edu/policies

Topic: Information Security/Protection of Data

1. Does your department or school have specific policies and standards regarding information security and the protection of sensitive data?

2. Do your policies and procedures include safeguards to prevent unauthorized physical access to sensitive data?

3. Do departmental policies or procedures include an exception process that covers deviations from the policy defining what may be considered an acceptable alternate security control and including a documented risk acceptance approval/escalation process that includes approval from the Dean/Director/VP/or AVP ?

4. Do the departmental policies include awareness efforts so that existing employees are reminded and new employees are made aware of them? Is this process tracked so that in the event of a breach the necessary documentation demonstrating the awareness efforts could be obtained?

Sensitive Data Handling and Access

1. Are there policies or standards documenting roles and responsibilities for anyone handling sensitive data? Are these roles and responsibilities reviewed and validated on at least an annual basis?

2. Does the department have policies and procedures for granting or removing access when employees are hired, transferred or terminated?

3. Do departmental policies address the security of data storage, data in transit and approved methods for data destruction?

4. Do you have a policy and procedure that defines when to use encryption and the approved methods for encrypting sensitive data?

5. Do you have a policy requiring appropriate agreements or contract language for 3rd parties with access to sensitive data? Are these contracts reviewed regularly?

Incident Response

1. Are there policies and procedures that define an ‘information security incident ‘and reporting procedures and responsibilities?

2. Are there policies and procedures to address security incidents, and does it include emergencies or damage to systems containing sensitive data?

3. Do you have a procedure for restoring sensitive data appropriately and are these procedures tested regularly?

HIPAA Specific (Most of these can also be found in NIST Standards and are considered best practices)

1. HIPAA Specific: Do you have a policy and procedure to prevent, detect, contain and correct security violations?
2. HIPAA Specific: Do you have policies and procedures to apply appropriate sanctions for failure to follow security policies and procedures?
3. HIPAA Specific: Are there policies and procedures to document modifications to user access to sensitive data?
4. HIPAA Specific: Do you have a procedure to regularly review records of information system activity such as audit logs, access reports and security incident tracking reports?