

Information Security Office

InfoSec Policy at UofL

Where we were

Where we are

Where we are going

Bruce W. Edwards, CISA, CIA, FLMI
Information Security Officer
University of Louisville

Bruce.EdwardsJr@louisville.edu
security.louisville.edu

College Of Business - CIS 481 - Fall 2005
Tuesday, November 22, 2005



Where we were

Information Security Policies, Standards and Procedures:

- Disjointed
- Hap-hazard
- Delineation between Policy, Standard, Procedure not always clear, not consistent
- Each policy evolved “organically” to fit a perceived need at the time (not a structured approach)

Where we were

Information Security Policies, Standards and Procedures:

- Not part of a cohesive, consistent and unified package
- Not organized, no clear overarching “Why” to what is there
- Hard to find
- Not effectively communicated to all constituents
- Policies written/implemented in a manner *not* conducive academic constituent support

Information Security Office InfoSec Policy at UofL

Where we were

Information Security Policies, Standards and Procedures:

- No possibility within policy of the possibility of self-direction (with regards to technology) within a structured framework
- Unclear and/or inconsistent sanctions
- Sanction enforcement, what is that?
- Unclear Senior Management Support
- Highly variable support within the organization (sometimes bordering on antipathy)

Where we are

- Support from Senior Management: Have achieved support from Senior Management for revamping policies into a consistent, cohesive whole
- “Radical” approach (for UofL) for this cohesive whole
 - * As ***technology neutral*** as possible
 - ~ Policy defines expectations for a technology but not the specific technology that must be used

Where we are

- Received support for consistently enforced sanctions

- Policy defined as:

* High level statement or short paragraph regarding a type of technology or behavior in the IT environment.

~ *Example Policy* ~

Policy Name: Protection from Malicious Software

Policy:

* “Malicious software (viruses, worms, trojans, root kits, hostile active X controls, etc.) must be actively guarded against within the University network using University approved tools. All computers must be configured with appropriate safeguards against malicious software.”

Information Security Office

InfoSec Policy at UofL

Where we are

-Standard defined as:

- * Descriptive guidance (but not step by step procedures) on how technology should be configured and deployed or descriptive guidance for a behavior based policy.

~ **Example Standards** ~

Standard Name: Protection from Malicious Software

(General or “over-all”) :

- * “Anti-virus, anti-spyware and firewall software must be deployed on all workstations, portable computers, and servers that attach to the University networks. Servers behind a properly configured hardware firewall and meeting other enterprise class configuration, administration and maintenance requirements may be exempted from some of these requirements (only as approved by central I.T.)”

College Of Business - CIS 481 - Fall 2005

Tuesday, November 22, 2005

Where we are

~ *Example Standards* ~

Standard Name: Protection from Malicious Software

(Technical)

- * “Only anti-virus, anti-spyware and firewall software as identified and approved by central I.T. is authorized for use.”
- * “All workstations and personal computers (PCs), including portables and systems used off-site, must be configured for automatic virus detection and spyware blocking.”

(Administrative)

- * “Managers must ensure that all desktops and systems in their departments have implemented the appropriate virus protection, anti-spyware and firewall controls as outlined in this document.”

Where we are going

- **Beginning process of achieving feedback and/or buy-in from appropriate University constituent groups** (faculty, staff, student representatives to the Academic Technology Committee, for example).
- **So UofL will be...**
 - ~ An organization with consistent, cogent policies that will both “pass muster” in the event of a regulatory review or audit and allow reasonable flexibility for technology implementations while maintaining information confidentiality, integrity and availability.

Information Security Office
InfoSec Policy at UofL

Thank you!

Bruce W. Edwards, CISA, CIA, FLMI
Information Security Officer
University of Louisville

Bruce.EdwardsJr@louisville.edu
security.louisville.edu