**IT28 Comprehensive Evaluation**

Unit Name: Click here to enter text

Unit Head: Dean, Executive Director, etc.

Submitted By: Click here to enter text

Submission Date: 5/1/2014

Table of Contents

[Executive Summary 3](#_Toc366837989)

[Overview of Unit Mission 3](#_Toc366837990)

[Overview of IT Services 3](#_Toc366837991)

[Risk Assessment – Brief Narrative 3](#_Toc366837992)

[Risk Mitigation Plan 4](#_Toc366837993)

[Risk Mitigation Timeline 5](#_Toc366837994)

[Risk Acceptance – Brief Narrative 6](#_Toc366837995)

[Concluding Remarks 7](#_Toc366837996)

[Signatures 7](#_Toc366837997)

# Executive Summary

Not required, but you can use this section if you wish.

# Overview of Unit Mission

Provide a brief description of what your unit does and who it serves. If administrative or clinical, does it collect payments from students or patients? If academic, does it have a graduate program?

# Overview of IT Services

How is the IT department managed and organized? What’s the ratio of IT staff to supported devices? Are personal laptops and mobile devices supported? Are students supported? If servers are kept on premises, describe the location and physical controls applied to server and IT equipment.

# Risk Assessment – Brief Narrative

What are your current security practices? Identifying where the gaps are between what you currently do and what you should be doing will help with your mitigation planning. The table below is a list of recommended and required best practices.

|  |  |  |
| --- | --- | --- |
| **Best Practices, Recommendations, and Requirements** | **Governing IT Policy or Standard** | **Currently Practiced or Planned?** |
| **Authentication** |   |  |
| Admin accounts not used for day-to-day activities | IT-12 |  |
| Users are not allowed to run systems as administrators | IT-12 |  |
| Admin accounts not shared among individuals - unique admin accounts/passwords for each  | IT-12 |  |
| Employ strong authentication requirements | IT-12 |  |
| Provide access to IU systems and services only to those authorized to access such services | IT-12 |  |
| Secure management of passwords | IT-12 |  |
| All mobile devices require at least a 4-digit PIN | IT-12.1 |  |
| **Backups** |  |  |
| All institutional data are backed-up; tests of backups routinely conducted | DM-01 |  |
| Maintain off-site backups | COBIT 4.1 DS4.9 |  |
| **Documentation** |  |  |
| Data stored or shared with third party is appropriately documented | DM-02 |  |
| Data stored or shared with third party is approved by Data Stewards | DM-02 |  |
| Up-to-date risk mitigation plan | IT-28 |  |
| Business continuity plan up-to-date | COBIT 4.1 DS4 |  |
| DRP formally tested | COBIT 4.1 DS4 |  |
| Inventory of IT assets, with data classifications, and data analysis | IT-28 |  |
| Written incident response procedure | IT-12 |  |
| DRP maintained and routinely updated | COBIT 4.1 DS4 |  |
| Formally assign roles of security and privacy | ISPP-25 Standard |  |
| **Physical infrastructure/hardware** |  |  |
| Offsite backups with critical data properly secured | IT-12 |  |
| Server room environmental controls are sufficient | DM-01-s  |  |
| Server room physical controls are sufficient | DM-01-s |  |
| Procedure for equipment decommissioning (i.e. hard drive-wiping, shredding) | FIN-PUR-14.0  |  |
| **Scans and log monitoring** |   |  |
| Regular (at least monthly) vulnerability scans on all servers | IT-12 |  |
| System logs regularly reviewed | IT-12 |  |
| System logs archived securely, and for the appropriate duration | UISO Recommended |  |
| Identify Finder scans routinely occurring on servers | DM-01 |  |
| Identify Finder scans routinely occurring on workstations | DM-01 |  |
| **Patch management, software, system builds** |  |  |
| Routine and consistent procedures for patch management | IT-12 |  |
| Servers on supported operating systems | IT-12 |  |
| Run systems with only necessary software, services and port openings | IT-12 |  |
| Identify and patch third-party software on systems | IT-12 |  |
| Mobile devices on IU’s network secured and managed | IT-12.1 |  |
| Maintain updated OS builds for efficient recovery | IT-12 |  |
| **Firewall, antivirus, encryption, network** |  |  |
| All servers behind physical firewall | DM-01 |  |
| Antivirus scans taking place on all systems | IT-12 |  |
| Critical/Sensitive data encrypted in transmission | IT-12 |  |
| Critical/Sensitive data encrypted at rest on servers | IT-12 |  |
| Encrypt communications to systems accessed through elevated privileges | IT-12 |  |
| Avoid whenever possible passing password over the network in clear-text | IT-12 |  |
| Antivirus software installed on all computers and servers | IT-12 |  |
| Maintain antivirus definitions  | IT-12 |  |
| All laptops employ whole disk encryption | IT-12.1 |  |
| Backup media on servers encrypted | IT-12 |  |
| All servers on private IPs (unless documented operational necessity) | IT-12, DM-01 |  |
| All printers on private IPs | IT-12, DM-01 |  |
| Disable or secure remote access | IT-12 |  |
| **Certifications / training / handling of sensitive data and security** |  |  |
| Hire technicians with the expertise necessary to maintain systems and hardware | IT-12 |  |
| Identify types data in your unit | DM-01 |  |
| All employees participate in security/privacy awareness (HIPAA/FERPA certs) | Health Insurance Portability and Accountability Act; Family Educational Rights and Privacy Act |  |
| PCI DSS compliance | [FIN-TRE-VI-110](http://policies.iu.edu/policies/categories/financial/treasurers-office/FIN-TRE-VI-110-accepting-electronic-payments.shtml) |  |
| Sensitive data managed on secure systems, by appropriate procedures and personnel | DM-01 |  |
| Training procedures in place for appropriate use and access to electronic information | IT-07, IT-12 |  |
| Subscribe to vendor advisory services | IT-12 |  |
| Keep abreast of IU security advisories, Policy and best practice updates through Secure IU | IT-12 |  |
| For users, identify appropriate server locations of data extracted or derived from central sources | DM-01, section 10.e |  |

# Risk Mitigation Plan

Provide a general narrative describing planned mitigation actions. Remember, even if every server was in the Intelligent Infrastructure, your unit must still maintain the operating system, firewall settings, and access controls. How are you keeping that inherent risk to a minimum? This isn’t just about server administration. End users can make mistakes. How are you making users aware of their responsibilities? Are you fully staffed to properly secure unit-level IT systems?

Because a risk mitigation plan for each individual IT asset is not practical, the table below assumes that similar risks are handled with the same control measures across similar IT systems. Notice in the examples below that you have rows 1a and 1b, both of which describe mitigation plans and current measures for the same risk (exposure of data due to hacking). The difference between the two rows is in the response action and subject of those response actions.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Risk | Response Action | Current Responsibility | Future Responsibility | Target Date |
| 1a. | Exposure or loss of university data (all classifications) due to hacking | **Workstations**: Will implement central patch management | IT Systems Manager | IT Systems Manager | May 15, 2014 |
| 1b. | Exposure or loss of university data (all classifications) due to hacking | **Workstations** and **servers**: will ensure all research data is copied to SDA | IT Systems Manager | UITS | September, 2014 |
| 2a. | Exposure or loss of university data (all classifications) due to theft | S**ervers: all** will be housed in the data center, incl. test & development servers. | IT Systems Manager | UITS | June 30, 2014 |
| 2b. | Exposure or loss of university data (all classifications) due to theft | All **laptops** use full disk encryption | IT Systems Manager | IT Systems Manager | July 31, 2014 |
| 3. | Exposure or loss of university data (all classifications) due to human accident or error | **Web content** providers will be properly and regularly trained; will train **researchers** to keep 3 copies of their data utilizing SDA, RFS, and/or local copies | IT Support Coordinator | IT Support Coordinator | April 15, 2014 |
| 4. | Exposure or loss of university data (all classifications) due to physical cause or accident | All **servers** will be housed in the data center, incl. test & development servers. | IT Systems Manager | UITS | June 30, 2014 |
| 5. | Interruption of mission-critical IT services or campus infrastructure due to physical cause or accident | All **servers** will be housed in the data center, incl. test & development servers. | IT Systems Manager | IT Systems Manager | June 30, 2014 |
| 6. | Loss of employee productivity due to malware or hacking event | **Workstations**: Will implement central patch management | IT Systems Manager | IT Systems Manager | May 15, 2014 |
| 7. | Other threat (please describe) |  |  |  |  |

# Risk Mitigation Timeline

Use this section to make special notes about the mitigation plan, since space is limited in the table above. What issues affect your mitigation timeline, particularly timelines that go beyond 12 months? Are you waiting for a license to expire? Are you waiting for the next budget cycle to hire an additional IT staff person? Are there any services you are providing that negatively impact your ability to mitigate risk, or to do so in a timely fashion?

# Risk Acceptance – Brief Narrative

Some risk may be unavoidable. Is there any risk that your unit accepts without mitigation? An example might include data collected on a special scientific instrument at a remote field station, which cannot be downloaded in the field. If that instrument were lost before being returned to the lab, all data would be lost.

# Concluding Remarks

Is there anything else you would like to make known?

# Signatures

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unit Head (signature) Printed

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT Manager, Director, or Delegate (signature) Printed

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date