University of Florida Health Science Center Security Audit

Conducted by: Akvile Kiskis, Arvin Bahrami, Dennis Chase, Karthik Ravichandran, Meghana Reddy, and Sean George (Team Yellow)

Executive Summary

The yellow team completed an audit on the University of Florida SPICE Policies as well as the IT Security Regulations policies to ensure that they fall under industry standards. The audit was performed in pieces by November 30th, 2017 and this presentation will outline the scope and findings from our audit.

Scope

The scope of our audit is to see if the Information Technology and Healthcare Information Security Policies of the University of Florida comply with the industry standards. Specifically, we will focus on five categories: general provisions, contingency planning, incident response, physical security, and technical security. In addition, we will audit IT Security Regulations Policies from the categories of: acceptable use, internet privacy, purchasing/E-Commerce, student computing requirements, identity and password, and networking.

SPICE Policies

https://www.healthit.gov/sites/default/files/Security_Shield_Lock.png

General Provisions

Findings:

All of the policies under general provisions have been updated lately to current standard with the exception of an assessment test. They need this in place so that all of the authorized employees who need access to this sensitive information can be updated frequently with latest threats and solutions. Our recommendation would be to have assessment test every six months in order to continue to have the access privileges to the employees.

Contingency Planning

Findings: The policy is up to par with the exception of the data center being tested within the last 12 months. The issue is that there was no finalized policy found, however there was a draft policy available for viewing. Unfortunately, the draft did not mention the data center being tested at all. Our recommendation would be to create a finalized policy and use the draft as a template; with this in mind, it is imperative that the finalized version include a standard for testing the data center within the past 12 months.

Incident Response

Findings: Currently, this policy is majorly flawed. The University of Florida currently has no Incident Response documents for the Healthcare Information Security Policies. All of the current links within the Incident Response are duplicates of the Contingency Planning documents without the updated relevant information. It is stated that this policy and associated standards will soon be replaced and are pending approval, so they may be aware of this issue, but have yet to fix it. Our recommendation is to create documents for the Incident Response policies.

Physical Security

Findings: Most of the Physical Security policies are inadequate. Many sections are missing information such as policies for: after-hours access, audit logging and monitoring, procedure for confidential information and disposal, and remote access. Versions of the Physical Security were last updated in 2010 and were labeled to be reviewed and replaced by 2012. This seems to have either not happened or the University just hasn't put up the most recent policies. These policies are labeled to be replaced soon and pending approval. Our recommendation would be to update these policies so that they are not half a decade behind and focus on user access and audit logging and monitoring specifically.

Technical Security

Findings: Some policies related to logging activities, contingency plan and malicious software controls did comply to the standards. However, some of the policies such as electronic communications and data transmission did not meet the standards. Policies like user account and password management and portable device computing were last updated in 2005 and 2007 and were labeled to be reviewed, but still not updated. The university needs to update these policies to ensure adherence; some recommended suggestions are to use standard encryption techniques like RSA when transmitting data across the network to keep the data secure and prevent from vulnerabilities.

UF IT Security Regulations Policies

https://www.host-logic.co.uk/wp-content/uploads/2016/09/it-security-surrey.jpg?quality=100.3017070710590

Acceptable Use Policy

Findings : The policy is up to par with regards to acceptable use policy in these ways :

1. User accounts and passwords are not shared among others.
2. There are procedures for monitoring of IT resources based on approvals.
3. Occasionally commercial use of IT resources is allowed.

Unfortunately, the policy was not up to par in this way:

1. Users can set up routers, switches, and WAPs.

Web Related : Internet Privacy Policy

Findings: The policy is up to par. It has been observed that the university abides by the policy too in terms of collecting information from children, it mentions guideline for parents to monitor their kids, most of the university official web sites follow the policy's quotes to provide a reference to the policy at the footer of the page. Pages on the university website are user specific, all users have different user interface.

Purchasing/E-Commerce & Student Computing Requirements

Purchasing/E-Commerce
Findings: Since there is no platform offering online payments or e-commerce, there is no need for the assessment of their policies and their relation to standardized procedures. The payments are all made either through customer insurance cards or in office if chosen to self pay.

Student Computing Requirements
Findings: It was mentioned that there are more specific student computing requirements based on each college. The requirements didn't change much for non IT related majors; for the IT students there were more requirements and there was a higher level of requirements technologically.

Identity and Passwords & Networking

Identity and Passwords
Findings: All the policies and regulation with respect to Identity and Password are up to standard except that they need to be updated regularly.

Networking
Findings: The policies in the networking section are incredibly slim considering it only has Internet Protocol Address Assignment Policy and Wireless Network Policy. These were last changed in 2013 and 2011 respectively and it is our recommendation that these should be updated when they get the chance.

Questions?