School of Applied Technology
ILLINOIS INSTITUTE OF TECHNOLOGY

Information Security Audit Report

University of Florida

November 30, 2016

School of Applied Technology
ILLINOIS INSTITUTE OF TECHNOLOGY

Table of Contents

School of Applied Technology
ILLINOIS INSTITUTE OF TECHNOLOGY

Executive Summary

This report contains the results of our audit of the University of Florida's IT Security domain. We, the Cyan Team, performed the audit on several important policies that fall under information security. After reviewing and comparing the policies to industry standards the team gave recommendations on what may need changing and reasons why the change is needed. The audit was then performed on November 30, 2016.

Background Information

Background

The university website handles many important and confidential information of students. Many students visit and stay updated regarding any important announcements through this source. Students can find links to the university's different policies especially the security policies as well. The security program is known as SPICE (Security Program for the Information and Computing Environment) of the University of Florida Health Science Center. Students may also access the Standard Lifecycle, Acceptable Use, Accessibility, email, information security, identity and passwords, intellectual property, networking, purchasing and e-commerce, and any other web-related links as well through this site. Students can also use these links to find other related standards and documents for each major policy in place.

Audit Objectives

The primary purpose of the audit is to assess the effectiveness and efficiency of security measures and their compliance, followed by University of Florida IT infrastructure. The objective would be focused on the IT Security domain of the IT infrastructure. The objective of this audit may also discuss any vulnerabilities and insecurities of the security measures that could also be found from HIPAA violations as well. Strengths will also be looked at as well as any omissions or weaknesses that may be found from the security measures. The audit will also look at how the times of policy transition could have also led to an increased vulnerability in the security measures and their compliance that is in place.

Scope

To assess if the institute's IT infrastructure complies with security best practices by following various security standards like National Institute of Standards and Technology (NIST), ISO 27000 series, HIPAA, etc. We have chosen to audit the university's Information Security, with each team member taking two sections of policies and standards.

Testing Approach

The audit was initiated with a short list of the important policies that could impact the infrastructure. Once the shortlisting was done, the entire team worked on creating a checklist, which worked as an aid for conducting the audit. Each member took a look at the sections they had chosen within the domain,each while reviewing the industry standards (NIST, ISO, OWASP, etc) and comparatively

noted any successes and discrepancies. Lastly, members compiled a recommendations list based on those successes and failures. A table was created (see below) where the information was compiled.

Findings, Observations, and Recommendations

Password Complexity Standard

System Security Plans

Authentication Management Policies and Standards

Data Classification Guidelines and Standards

Account Management Policy and Standard

Risk Assessment Standard and Management Policy

Mobile Computing Storage Devices and Backup Recovery Standard

Sr no.	Area	Compliant?		Findings	Recommendations
		Yes	No		
1	**Password Complexity Standard**				
1.1	Is minimum length of password 8 characters?	Yes		The minimum password length is 8 characters, which is a good security practice.	
1.2	Is maximum password age 30, 60, or 90?		No	The password maximum age is 365 days and 180 days in some cases.	This is not secure and it must be changed to either 30, 60, or 90 days.
1.3	Is account locked out after 3-5 invalid attempts?		No	The account gets locked out after 10 invalid attempts.	This policy should be updated and kept to 3-5 attempts.
2	**Policy: Backup and Recovery**				
2.1	Are backups periodically tested?	Yes		The policy states that backups are periodically tested to ensure that everything is sufficient and reliable	My recommendations for both findings is that the references are updated. The reference is to NIST 800-53 revision 3 that was updated August 2009 but there is a current SP 800-53 Rev. 4 last updated 1/22/2015
2.2	Are there procedures in place	Yes		Mentions that there are written procedures in place	The policy in general is short, maybe include more

	to recover data in case of an emergency?			and includes the responsibility of different IT security admins and managers on how to handle the backup and recovery systems	information but other than that it looks fine.
3	**Mobile Computing and Storage Devices Policy**				
3.1	Is there a system in place that states data should be encrypted?	Yes		The policy does state that Restricted Data stored on mobile computing and storage devices should be encrypted.	My recommendation would be for the policy to reference another source that they are basing their own policy on. The only references listed are their own definitions and standards. My recommendation would be for this policy to reference the NIST 800-124 Rev. 1 on the Guidelines for managing the Security of Mobile Device in the Enterprise.
3.2	Does the policy state that desktop computers must follow the mobile computing policy?	Yes		Yes, there is a mention that desktop or workstation computers must apply to this policy	It includes thorough responsibilities on how to handle this but it should reference another source besides their own as stated in the above recommendation.
4	**Policy & Standard : Account Management**				
	Does the system automatically disable inactive account after organization-defined time period?	Yes		The Standard referred that accounts not used within 180 days are to be disabled, and explicitly re-enabled prior to further use. Temporary accounts should be issued with a pre-set expiration date.	It is satisfied NIST requirement because they define a time period (180). But The period in the standard should be controlled by role specifically like Disabling the user identifier after ninety (90) days of inactivity for general user accounts and thirty (30) days for administrator level accounts. The reference is to

					NIST Special Publication 800-53 AC-2(3).1 (Rev. 4)
	Is there a automated mechanism to audit account creation, modification, disabling, and termination actions?	Yes		In the policy, There is a mechanism to be promptly modified upon changes in university affiliation, position, or responsibilities. According to Standard, Accounts and authorizations must be promptly modified when the assigned user's job duties or assignment change, or upon termination of employment or appointment.	This policy is mentioned generally no specific plan. I would like to recommend to make details prepared for several cases like conflict of duties
5	**Risk Assessment Standard & Risk Management Policy**				
5.1	How often does the Organization assess the risks?	Yes		Assessments must be completed prior to purchase of, or significant changes to, an Information System and assessed for risk every 2 years	Policy is Appropriate, but recommend risk assessment to be once a year, due to importance of medical equipment.
5.2	What are the steps for an assessment	Yes		1. The scope of the assessment. 2. An assessment of security control implementation. 3. Report documenting threats, vulnerabilities and risks associated with the Information System. 4. Recommendations to increase the security posture of the Information System.	The Standard: ID the threat What may be harmed Chance of threat happening Record the findings The steps are compliant, but recommend monitoring to be added to ensure threats are neutralized and no longer occur
6	**Authentication Management and Standards**				
6.1	Are passwords protected?	Yes		• The policy states that the passwords are always stored in encrypted form rather than cleartext. • As the data access is restricted due to segregation into levels, every level has a	The lower levels P1and P2 are less protected and can use two factor authentication method to authenticate users.Apart from that the levels are secured with latest authentication methods.

				protection procedure per sensitivity. • The standards also mentioned about the encryption of passwords when transmitted over a network. • The standards also mentioned about what happens when the passwords are reset over mobiles and other devices by verifying their identity using on-public information. • The standards also mention about taking special measures to run periodic tests which are disposed or automatically expired when they find that they are in violation	
6.2	Is the privacy policy made clear to every user?		No	The policy states that whenever a user is given a new account or change the password after a period of time , the user is made to read the acceptable use policy before updating to a new password.	If the privacy policy is animated(say a video showing different scenarios and steps to be taken) instead of huge paragraphs, will ensure better knowledge to the user about policy.
7.0	**Data Classification Guidelines and Standards**				
7.1	Do Classification Standards contain at least Public, Business, and Classified cases?	Yes		Open [Public] Sensitive [Business] Restricted [Classified] They require the explicit approval of the owner of the information, even if the classification is delegated to another individual or group.	A low priority recommendation would be to separate faculty and student information, but overall this policy meets requirements.
7.2	Complete and thorough documentation in an appropriate location?		No	While the actual guidelines were easy to find, there was so documentation on remediation, prevention, and punishments for the information. For example, how many strikes does an employee get for emailing out sensitive information?	Strongly recommend documenting at least general remediation and prevention techniques, as well as having expected outcomes in writing so that there can be no wiggle room.
8	**System security plans standard**				

8.1	**Do security plans need to be approved?**	Yes		The security plans are reviewed and approved by information security administrator and information security manager.	
8.2	**Is information classified before saving?**	Yes		The information classification f data is done before saving any documents.	
8.3	**Are security plans updated regularly?**		No	The security plans are updated after minimum 3 years.	The plan should be updated regularly to avoid any security gaps.

Conclusion

After thorough analysis of policies, we conclude that there are some policies which are not implemented securely. This leaves UFL'S infrastructure vulnerable to malicious activities. Hence, we have proposed some recommendations to implement these vulnerable policies.

School of Applied Technology
ILLINOIS INSTITUTE OF TECHNOLOGY

Reference List

Hayes, b. (2015, July 1). Tips for creating a data classification policy. Retrieved December 7, 2016, from http://searchsecurity.techtarget.com/feature/Tips-for-creating-a-data-classification-policy

In-line Citation:(Hayes, 2015)

Security and Privacy Controls for Federal Information Systems and Organizations. (2013, April). Retrieved December 7, 2016, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

In-line Citation:("Security and Privacy Controls for Federal Information Systems and Organizations," 2013)

Souppaya, M., & Scarfone, K. (2013, July). Guidelines for Managing the Security of Mobile Devices in the Enterprise. Retrieved December 7, 2016, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

In-line Citation:(Souppaya & Scarfone, 2013)

Control. Retrieved December 7, 2016, from National Vulnerability Database, https://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=IA-5

In-line Citation:("Control," n.d.)

Best Practices for Privileged User PIV Authentication. (2016, April 21). Retrieved December 7, 2016, from

http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

In-line Citation:("Best Practices for Privileged User PIV Authentication," 2016)

Password strength (2016). . In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Password_strength

In-line Citation:("Password strength," 2016)

ISACA. (2014). Retrieved December 7, 2016, from http://www.isaca.org/Journal/archives/2014/Volume-2/Pages/JOnline-Reinspecting-Password-Account-Lockout-and-Audit-Policies.aspx

In-line Citation:("ISACA," 2014

Account Management | Disable Inactive Accounts. Retrieved December 7, 2016, from https://compliance.cloud.gov/standards/NIST-800-53-AC-2%203.html

In-line Citation:("Account Management | Disable Inactive Accounts," n.d.)

Control. Retrieved December 7, 2016, from National Vulnerability Database, https://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=AC-2

In-line Citation:("Control," n.d.)