Information Security Audit Report

University of Florida Health Science Center

Silver team

Arianit Pajaziti
Dipen Delvadiya
Jean-Claude Rock
Moses Alade
Ramya Chowdary Chadalawada
Yanhao Zhang

ITMS 478/578 - Cyber Security Management, Fall 2016

December 1st, 2016

EXECUTIVE SUMMARY

A document audit of the Information Security program for the University of Florida Health Science Center was performed. The Information Security program of UF consists of a series of policies, standards and guidelines that must be fulfilled by its employees. This program represents a set of strategies for preventing, detecting threats against UF's data and information. Information Security program of UF is composed of a group of six sub-fields, namely the Mobile Computing and Storage Devices; Data Classification; Authentication Management; Risk Management; Account Management; Backup and Recovery. The corresponding policies and guidelines for can be found in the UF's web-page [5]. As there was no onsite visit, the audit was conducted only based on the information found in the policies and other documents in the UF's webpage. It is assumed that the rules stated in the policies are strongly complied by the UF staff. It must be stated that the documents are not very well organized in the webpage, and many of the links are broken, so once clicked they display an error. A checklist was designed by the team for controlling the various aspects of the Information Security program of UF. The checklist was created as a result of a research from various audit reports found online and the standards from the National Institute of Standards and Technology [6]. A comparison of the information found in the policies in place and the checklist was performed, thus leading to the audit results.

FINDINGS, OBSERVATIONS, AND RECOMMENDATIONS

Mobile Computing and Storage devices

Responsible person: Jean-Claude Rock

The University of Florida (UF) has two documents that define and regulate the mobile computing and storage devices policy. These documents – Mobile Computing and Storage Devices Policy [1], and Mobile Computing and Storage Devices Standard [2] – are used to conduct the audit on Mobile Computing and Storage Devices subsection. The purpose of the audit is to identify the existence and operating effectiveness of security controls over selected mobile devices designed to protect the UF data, and to assess the adequacy of campus mobile computing security policies, risk assessment, and governance. A checklist (Appendix A) is used for investigating the Mobile Computing and Storage Devices Policy, and the findings are as follows:

- There is no information about unclassified mobile devices in use at the University of Florida, and we believe that there may not be any unless special authorization has been given to such users in compliance with University of Florida Information Security Policies and Standards to the mobile computing use policy. However, if there is a report that unclassified mobile devices are in use on the university area, specific action must be taken.

Recommendation: Based on Policy SC-TS-05, the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information should be prohibited unless specifically permitted by the authorizing official.

- There is no information that anyone has received the permission to use unclassified device at the University premises. If this is the case, there should be a compliance to the University of Florida Information Security Policies and Standards to the mobile computing use policy.

Recommendation: Policy SC-TS-05 recommends that the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information should be prohibited unless specifically permitted by the authorizing official.

- The university policy prevents the use of Restricted Data on a mobile computing device unless a permission has been first obtained from the Data Principal. In this case, the amount of Restricted Data and the length of time the Restricted Data is used are minimized.

Recommendation: Policy SC-TS-05 recommends to enforce the following restrictions on individuals permitted by the authorizing official to use unclassified devices in facilities containing information systems processing, storing, or transmitting classified information: restricts the connection of classified mobile devices to classified information systems in accordance with the University of Florida security policies.

- The UF policy recommends that all portable storage devices must be fully encrypted. The encryption and key management methods used must have the approval of the UF Chief Information Security Officer. Restricted Data must be protected by encryption during transmission over any wireless network.

Recommendation: Policy TS05.01 recommends to use full-device encryption to protect the confidentiality and integrity of information on the UF defined mobile devices.

- The UF policy does not give any specific of using container encryption to protect classified data on all portable storage devices.

Recommendation: Policy TS05.01 recommends to use container encryption to protect the confidentiality and integrity of information on the UF defined mobile devices.

Data classification

Responsible person: Moses Alade

The policies described the classifications of data respectively and it also addressed the criteria for which an information has been classified. We have the restricted data which are data that are subject to specific protections under federal and state law. HIPAA also defined the standard for which information can be restricted or open depending on who needs and when the data is needed. In addition, we have sensitive data which are but not limited to research work in progress and Open Data which are information that anyone can have access to. All the requirements must be met before a data can be included in the either of the category.

Recommendation: Even though the University has its own standard for classifying data/information. It is highly recommended that the HIPAA and FERMA rules are strictly adhered to. The organization should also keep itself updated periodically about the rules and regulations. It must also be ensured that past employees must not have access to restricted or sensitive information. Any information that will be transferred to a third party must be done with the permission of the concerned individual and must go through proper screening and authentication. It must be ensured that data requested must be used for the purpose it is requested for.

Authentication Management

Responsible person: Dipen Delvadiya

The University of Florida has a large amount of sensitive data of all the students and instructors. University gives access to only permitted users with limited authentication access depending on the type of user. The passwords are the primarily mean of accessing any computer or data. It is essential for passwords to be strongly constructed. People are strongly recommended not to share any passwords with anyone. The University is in possession of Authentication Management policies, whose purpose is to manage authentication access and assure the quality of the passwords.

Policies SEC-AC-002.01 and SEC-AC-002.02 define the standard of authentication management and password complexity respectively. Everyone must meet the minimum requirements to get into the network. Defined policies can handle any low-level attack, but their certificates of the standard are three years old. They need to use latest programs and certificates to have high level standard of their defense against any experienced attacker.

Important Terms:

P1: Entry level. It provides an access to the basic university network, but no access to any sensitive information.

P2: Low level. It only provides an access about oneself, but no other access.

P3: Medium level. Accounts provide access to others' information and limited access to restricted data.

P4: High level. Accounts provide access to institutional and restricted data.

P5: Rigorous level. Account provide access of controlling institution.

Recommendations:

- Although SEC-AC-001 and 002 have different standard for ranging P1 to P5 it is highly recommended to have the latest and updated certificate standards for minimum P4 and P5.
- Policy SEC-AC-001 well defines the password complexity and automated tool to satisfy minimum needs. Same way, it defines the standard process of re-creating any password or P1 to P3 accounts. SEC-AC-001 clearly states that individual must log on before joining their devices with the network. Everyone is responsible for not sharing their data with anyone. However, anyone should not be allowed to attempt more than 3 times to log in to network, and if they try more than three invalid attempts, user must be noticed that his/her account is locked.
- Policies do not explain if organization should implement any safeguard to manage the threat due to same account on different devices. Individual must be allowed to log in to limited personal devices.
- Although policies are well defined in standards of quality and safety, but individual must be asked to log into system again after certain time due to more safety reasons according to IA-11.

Risk Management

Responsible person: Ramya Chowdary Chadalawada

The University of Florida is one of the most populated universities with 52,286 students. The huge amount of data is managed appropriately only when the risk is minimal. The university should review and update risk management strategy to address organizational changes. The purpose of risk management is to develop a comprehensive strategy to organizational assets, individuals and organizational operations.

Analysis:

The policies PM-9, RA-1 and RA-3 defines the standards of Risk Management Policy. The policy describes the patterns in which the risk assessment must be performed on various kinds of data. Risk identification methods must be accepted before placing the system into operation. The residual risk is accepted after appropriate evaluation by the Chief Privacy Officer and Chief Information Officer. Each information system must be encrypted with appropriate security plan. The systems that store restricted data are analyzed every 2 years. Identified risk will be accepted before placing into operation.

Responsibilities for officers in the organization

Information security officer should ensure that their team conduct the risk assessment after getting the approval from the university. Information security managers are responsible for mitigating and assessing risk with the university approval. Information security owners are responsible for transferring. Accepting or mitigating the risk that is assessed. If the risk is controllable or solvable then it is taken into consideration at this stage. Chief Information Officer is responsible for implementing systems with appropriate specifications aligning the policies.

Recommendations:

- All the standards must be met before the risk is assessed. The HIPPA and FERPA standards by which the risk assessment can be conducted are stricter and comprehensive.
- Information systems must be prepared and planned before any assessment takes place. HIPPA recommends to increase security posture. Though the organization follows the rules and regulations, it also needs to get updated simultaneously on the procedures and latest regulations.
- Although SEC-RM-001 has defined standards in higher range of level 4, it is better to have the updated versions of certificate standards.
- Policies don’t explain the scope of the assessment.
- The residual risk must not be accepted by the Chief Privacy Officer though the organization give the authority to deal with it.
- 2 years of time is late to update the information systems. Once in every 8 months the systems must be updated.
- Although policies are well defined in the standards the administrators, managers or officers must have the right to implement risk management strategy according to PM-9.
- Management commitments, coordination among the team must have been defined well in the policy according to RA-1 policy
- Organizational assessment of risk must be monitored and alerted when necessary.

Account Management

Responsible person: Yanhao Zhang

The University of Florida has account management policies, whose purpose is to provide a comprehensive account management process that allows only authorized individuals access to university data and information system. There is one main policy for account management, namely SEC-AC-001.

Establish Information System Account Management Baseline Control. Develop and define daily operations for Account security program management. Identify the types of information system accounts to support, such as student accounts, professors, maintenance, and administration. The system automatically audits the account Create, modify, enable, Disable, and delete operations.

Recommendations：

- If the account is misappropriated, it should have a timely complaint process. The policy doesn't mention it.
- Different accounts will have different permissions. The policy doesn't express provision for this article.

Backup and Recovery

Responsible person: Arianit Pajaziti

The University of Florida is in possession of two main documents in regards of Backup and Recovery. There is a defined Guidelines document [3], and a Backup and Recovery policy [4]. These two documents are used as the baseline for conducting the audit on the Backup and Recovery field. The goal of the Backup and Recovery controls is to assure that the University of Florida will be able to recover from a potential loss or destruction of UF Information System hardware or software. A checklist (Appendix A) is used for investigating the Backup and Recovery Policies, and the findings are as follows:

- University of Florida backs up the data sufficiently to restore a part or all the Information System Data in the event of original data loss. The policy SEC-CP-003 doesn't specify the Recovery Time or Recovery Point objectives of data. This information is decided by the ISAs in consultation with Unit users. It is the responsibility of the ISAs to verify that appropriate backup plans exist for each Unit.

Recommendation: Although policy SEC-CP-003 states the necessity for Data backup and clearly states the responsible persons for backup plan verification, it is suggested that this document is enriched with specific data backup periods, Recovery Times, and Recovery Points for specific organization Units.

- SEC-CP-003 policy clearly states that the confidentiality, integrity, and availability of backup information at storage locations must be protected. However, no description/guidelines are provided of how this process should take place. The guidelines document suggests the IT workers that the Restricted Data must be transferred outside of known facilities only encrypted.

Recommendation: Develop specific policies/rules that define encryption standards, and confidentiality levels for each specific Unit of organization. For the data that can be visible to anyone and where there is no need for encryption, it is suggested to define standards that describe the ways of maintaining the integrity of information.

- There is no specification in the policy or guidelines that describes the medium used for data storage for backup purposes. It is well defined in the guidelines document that storage locations and transportation is to be approved by the Data Principal (Dean, Director, or Department Chair), which represents a good protection measure.

Recommendation: Detailed information of how the backup data is stored and transferred should be developed. Although the guidelines suggest the IT workers that data should be disposed in a physically secure location, there should be a document that describes the characteristics of a secure location.

- Backups are periodically tested to ensure that backups are sufficient and reliable, also writing procedures are maintained to allow for data recovery by the Unit personnel.
- No controls are in place at the off-site storage location to ensure that it is fireproof and secure.

Recommendation: Implement document that specify the rules for off-site storage location.

- The organization doesn't specify any enforcement for dual authorization for the deletion or destruction of backup data.

Recommendation: It is recommended that for data classified as Restricted Data that special regulations are developed for ensuring that no backup data is destroyed without dual authorization.

CONCLUSION

Main conclusions drawn for each of the sub-fields from the Information Security program are as follows:

- Mobile Computing and Storage Devices: Although the policies are well implemented, improvement should be made for the use of container encryption for data protection.
- Authentication Management: Policies are well defined in current standards, but they should implement latest safeguard and certificates to make authentication process more secure.
- Risk Management: Policies are well defined, but HIPPA and FERPA standards which are more comprehensive must be followed to assess the risk.
- Data Classification: The University law, HIPAA, and FERPA must be strictly followed. The University must keep itself updated periodically about the rules and regulations
- Account Management: Additional permission information should be provided for various accounts.
- Backup and Recovery: The current policy and guidelines should be refined with more detailed specifications on backup plans, so that any inconsistencies are avoided

DEFINITION OF TERMS

Data owner: This is usually a senior employee that has attained a leadership level who his/her job is typically to protect and ensure that appropriate procedure is been followed when the university data is used. The data owner might be the dean, director, or head of department.

Data custodian: This is/are staff member(s) whose responsibility is to document the local process and procedure to ensure the safety of data. This is the person that is majorly responsible for IT and reporting the gaps on the processes to the data owner.

Data user: this is any member of the university community that has access to university data, and thus is entrusted with the protection of that data. They are capable detecting and preventing security breaches.

Unit: Any subdivision of the university independently responsible for complying with information security policies and standards; typically a college, department or institute.

ISA: Information Security Administrators

UF: University of Florida

Restricted Data: Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records, research protocols and export controlled technical data.

REFERENCES

[1] SEC-TS-05 Mobile Computing and Storage Devices Policy http://www.it.ufl.edu/policies/information-security/mobile-computing-storage-devices/

[2] TS05.01 – Mobile Computing and Storage Devices Standard http://www.it.ufl.edu/policies/information-security/mobile-computing-storage-devices/standard/

[3] UF Guidelines for IT Workers to Protect Restricted Data on Backup Media http://www.it.ufl.edu/wp-content/uploads/2012/10/it-worker-backup-guidelines.pdf

[4] Policy: Backup and Recovery http://www.it.ufl.edu/wp-content/uploads/2016/02/Backup-and-Recovery-Policy-v1.0.pdf

[5] Policies http://www.it.ufl.edu/policies/#security

[6] NIST https://www.nist.gov/

APPENDIX A

Mobile Computing and Storage Devices		
Requirement	**Document Reference**	**Findings**
Are there unclassified mobile devices in use at the University of Florida?	SC-TS-05	No information
Did anyone receive the permission to use unclassified device at the University of Florida?	SC-TS-05	No information provided
Are there any enforced restrictions upon individuals authorized to use unclassified device at the University of Florida?	SC-TS-05	Yes
Does the University of Florida employ full-device encryption to protect the confidentiality and integrity of information on mobile devices?	TS05.01	Yes
Does the University of Florida employ container encryption to protect the confidentiality and integrity of information on mobile devices?	TS05.01	No specific information
Data classification		
Is individual's identifiable health information protected and not released to unlawful individuals?	Data Classification Policy	Yes
Are student records properly secured?	Data Classification Policy	Yes
Are past students records properly secured?	Data Classification Policy	Yes
Does the organization have a policy to ensure former employees not use information they had access to in the past?	No information	No
Does the organization ensure that data released has been used for what it is meant for?	No information	No
Authentication Management		
Does the system enforce a limit of invalid logon attempts?	SEC-AC-002.02	Yes
Does the organization have an automated tool which tells users if the passwords are sufficient strong to satisfy?	SEC-AC-002.01	Yes
Does the software encrypt the password in case of transmission?	SEC-AC-002.01	Yes
Does the organization implement any safeguards to manage the threat due to individual having accounts on different systems?	IA-5(8)	No
Does the organization implement mechanisms to cryptographic module for authentication under the federal laws, policies, regulations, and standards?	SEC-AC-002.01	Yes
Does the organization require users to re-authenticate their devices at certain time-period?	IA-11	No

Does the system uniquely identify and authenticate before accessing to any restricted data?	IA-3 SEC-AC-002	Yes
Does the organization ensure that unencrypted users are not allowed to access any scripts or information stored in the function keys?	SEC-AC-002.02	Yes
Risk Management		
Does the organization conduct risk assessment prior to acquisition of information systems?	SEC-RM-001	Yes
Does the organization conduct risk assessment at least once in 2 years for existing systems?	GP0008	Yes
Is the risk assessment done for un stored data and restricted data at least once in three years?	SEC-RM-001	No
Is risk assessment completed before purchasing or changing to information systems?	SEC-RM-001	Yes
Does the organization submit a report on threats, vulnerabilities and risk associated with the information systems?	CP0002.02	Yes
Does the organization conduct risk assessment before changing the technology or updating to latest versions?	GP0008	Yes
Does the organization have a risk assessment scope?	NA	No
Does the organization assess security control implementation?	NA	No
Is the organization ready to accept recommendations to increase security posture of the information systems?	SEC-RM-001	Yes
Account Management		
Is the use of the enterprise authentication service by an application authorized by the Authentication Service Provider?	SEC-AC-001	Yes
Are the accounts for individual use with an academic or business need?	SEC-AC-001	Yes
Do student employees have separate accounts from their student accounts?	SEC-AC-001	No information
Do student accounts have student employee-related access?	SEC-AC-001	No information
Backup and Recovery		
Does the organization conduct backups of user-level and system-level information contained in the information system?	SEC-CP-003, Guidelines document	Yes
Does the organization protect the confidentiality, integrity, and availability of backup information at storage locations?	SEC-CP-003	Yes
Are critical files and programs regularly copied to tapes or cartridges or other equivalent medium to establish a generation of files for audit trail purposes?	SEC-CP-003	Partial information
Are the critical files removed to alternate/off-site storage to ensure availability in the event of a disaster?	SEC-CP-003	No clear information
Is a periodic inventory taken to verify that the appropriate backup files are being maintained?	SEC-CP-003	Yes
Are controls in place at the off-site storage location to ensure that it is fireproof and secure?	NA	No information

Does the organization test backup information periodically to verify media reliability and information integrity?	SEC-CP-003	Yes
Does the organization enforce dual authorization for the deletion or destruction of backup data?	NA	No

APPENDIX B - SCOPE

A document audit of the Information Security program for the University of Florida Health Science Center will be performed. This involves the investigation of series of policies, standards, and guidelines. Audit will be conducted based solely on the information found in the policies and other documents in the University of Florida's webpage. It will be concentrated in the Information Security program policies and guidelines. The main subfields of this program to be investigated are:

- Mobile Computing and Storage Devices
- Data Classification
- Authentication Management
- Risk Management
- Account Management
- Backup and Recovery

The audit will be started by creating a checklist that helps verifying the most important points of the policies. Based on the findings from this checklist, recommendations will be developed. The steps to be taken are as follows:

1. Checklist development
2. Investigate the policies/guidelines documents based on the checklist
3. Identify the results
4. Publish findings in a report
5. Provide with recommendations