ILLINOIS INSTITUTE OF TECHNOLOGY
School of Applied Technology

Security Audit Report

Prepared for:

University of Florida Health Science Center

Prepared by:

Silver "Protect" Team of ITMS 578

Timothy Kang, Satwik Gorre, Vinay Vijayakumar, Bolortuya Tumurbaatar,

Mallikarjuna Sirabadige Nagaraju, Reshma Jabeen, Erick Cabrera

Contents

Contents 2

Executive Summary 3

Findings 4

General Provisions 4
Contingency Planning 4
Incident Response 7
Physical Security 6
Technical Security 7
University of Florida Information Technology Security Regulations 8
Information Security and Emails 8

Conclusions and Recommendations 10

Appendices 11

Scope 11
Checklists 11
General Provisions 11
Contingency Planning 13
Incident Response 14
Physical Security 15
Technical Security 16
Information Security and Emails 18
References 19

Executive Summary

The silver team has been hired by Professor Ray Trygstad of ITMS 578 to conduct a security audit of the University of Florida's SPICE policies and IT Security Regulations policies. The targeted two sections are divided within the team to build the assessment. This audit will take into account how these policies comply with industry standards. The strengths and weaknesses of each of these policies are highlighted and a carefully curated checklist was prepared so as to clearly distinguish compliant and non-complaint sectors of the organization. To back each of these findings we have provided possible notes on the impact of non-compliant sectors on the overall cybersecurity strategy of the university. Our assessment solution will provide The University of Florida with assurance that the assessments provide better visibility into the status, progress, completion and results of the established security policy and help build a resilient ecosystem.

Findings

General Provisions

University of Florida's general provisions policies address information security definitions of terms, information security considerations, and violations, and also has a significant emphasis on security education.

Strengths:

- Robust data handling system.
- Strict university-wide regulations for infosec violations.
- Continually evolving protection process included with awareness training.
- Standard risk assessment policy.

Weaknesses:

- No network diagram to visually determine separation between ecosystems.
- Absence of formal approval process for data flows.
- IT Policy and Standard Life Cycle is missing/not found.
- Unavailability of vulnerability threat score or metrics.

Contingency Planning

University of Florida’s contingency planning policies address maintaining information during disaster, ensuring all requirements of the contingency planning policies are satisfied, determining which assets are absolutely necessary to the function of the unit, and to specify requirements of system backups. Contingency planning template is used to document the policies’ procedures noted above.

Strengths:

- Backups are done periodically.
- Plans reviewed and updated annually.
- Training conducted annually at each change.
- Annual reporting.
- The copies of information classified as restricted is retained offsite.
- Integrity and validity is verified to prevent unauthorized access.
- Each asset's value is determined for risk assessment.

Weaknesses:

- Does not cover if response plans are tested.
- There is no copy of the organization's risk assessment to ensure vulnerabilities.
- Risk assessment is reviewed every 2 years. The recommendation is every year.
- Unknown if confidential data stored in devices such as laptops or computer is encrypted or not.

Incident Response

University of Florida's incident response policies address protection of the security of information during disaster occurrence or other events resulting in loss of information assets. The incident response has multiple sub-categories: security Incident Response Team maintains security of information system, Information Security Incident Classification maintains confidentiality, integrity, availability and reliability of Information assets. The risk assessment evaluates which assets are vital to the functioning of the unit, and loss of it could be a risk to the unit.

Strengths:

- In case of disaster, implementation of contingency plan, and recovery process is in place.
- Contingency plan addresses disaster preparation, recovery of functionality after a disaster.
- A record maintained for crucial assets.
- Documentation of downtimes, outages, failures, data loss is recorded.
- Records are inspected by Information Security Managers.
- Plans and policies are reviewed and updated annually by CIO's.
- Documentation are backed up on offsite locations in case of data loss.
- Reviews and changes to the plan are stamped with date and time.
- Recovery process trainings are done annually.

Weaknesses:

- Where data is getting recorded is unknown.
- No records of risk assessment reviewed plans.
- It's not clear if only authorized personnel has access to data.
- No separation between restricted data containing system and normal system.
- Risk assessment conducted biannually.

Physical Security

University of Florida's physical security policies address the people responsible for establishing security requirements based on campus and type of assets, standards for physical access, security standards and guidelines for server rooms and communication closets, destruction of device and media controls, and access to end-user computing devices.

Strengths:

- Requirements are listed and categorized based on data type.
- Roles and responsibilities are well defined.
- Access to physical assets managed.
- Hardware and data destruction procedures are in place.

Weaknesses:

- Outdated (since 2010).
- Policy revisions not updated or still pending.
- Regulations on physical access not complete (ex: termination procedures).
- Specific end-user access regulations need to be defined.

Technical Security

The Technical Security is crucial to an organization which addresses many policies and the same thing has been implemented by the UF Health Science Center. It mainly focuses on securing the data resources being accessed in a standard format, risk assessment, security patch administration and it applies to all the systems connected to the University network.

Strengths:

- System/Activity Log is maintained in a timely manner.
- Strong emphasis with respect to authorization and level of access.
- Automatic logoff system activity in place when access to sensitive information session is inactive for a particular time.
- Systems implement malicious software control systems to ensure there is no corruptive data imported into the systems.

- Risk assessment results must be taken care of by making it less severe before the system is placed into operation.
- The key persons within the scope of the policy operating on the Universities credit card information storage and maintenance should complete a UF training module.
- Security patch management is taken care of by the system administrators to protect against the data breaches and malicious attack.

Weaknesses:

- Logs for a particular network part and input/output information activity are not clear.
- User accounts review over a duration of time to check for the level and scope of access are not defined.
- Logical controls such as VLAN and network defenses such as firewalls are not in place.
- The level and scope of access for the vendor accessing the resources is not defined by the Network service provider requirements.
- Mitigation strategy to handle the assessed risks is not explained by the Risk Assessment Policy.
- Procedure for removal of restriction information storage from the personal and user computer is not properly mentioned in the policy

University of Florida Information Technology Security Regulations

Information Security and Emails

The University of Florida's information security and email policies address how to keep data secure and prevent any breach or data loss. They specifically explain the part that each job role has in certain situations as well as their responsibilities to ensure the protection of data and the

prevention of data loss and breaches. These policies specifically outline what sort of measures to take when there is data loss. The policies also serve as a guideline when it comes to managing risk. They carefully explain what each person must do to ensure that all risk assessments are properly conducted and are successfully completed. The policies also cover a very important section when it comes to information security, handling emails. Emails have been a very popular way of breaching data and the university provides policies that help prevent these breaches and prevent time being wasted. These policies state how spam emails are handled and what kind of devices are allowed to access information within the university.

Strengths:

- Clearly states the responsibilities of specific job roles and users.
- Assessments are required before purchasing an Information System and are then required to be assessed every two years after.
- Data backups are periodically tested to make sure they are up-to-date and reliable.
- Mobile computing devices are required to be approved by the institution first and are secured by Information Security and Compliance Officers.
- An ufl.edu email is provided to all faculty and staff of the university and is monitored to ensure information safety.

Weaknesses:

- Not all policies are up to date as some were last revised six years ago.
- Examples of each data type of briefly explained, instead they should provide an extensive file or section with detailed examples of each data type to make it clearer.
- There is no required periodical assessment of personal mobile computing devices to ensure they are still compliant with encryption policies after initial set up.

Conclusions and Recommendations

In conclusion, there are many things that the University of Florida Health Science Center did right in terms of policies which can serve as a strength. But one thing this audit showed is that there are plenty of weaknesses too. While each weakness differs in scale, long and short term effects, and difficulty of implementing or fixing, they should all be addressed to mitigate as much policy related risks as possible. For example, policies should be completely visible and accessing them should be straight forward. However, some policies lead to dead links where they cannot be found. In addition, some policies are completely outdated despite their importance to the organization. It is great that topics like data classification and security awareness training are covered but specifics on things end-user access and certain security procedures should be given and emphasized. While this audit only covered the “protect” function, there are still many weaknesses that should be fixed before moving on to another function. By doing so, the policies will comply with industry standards and be strong in any kind of situation.

Appendices

Scope

The scope of this audit will only cover the "Protect" function of the NIST Cybersecurity Framework. This audit will assess the University of Florida's healthcare information security policies and information technology security regulations. The audit will be broken down into sections corresponding to how the policies were divided. Deprecated policies will not be audited. The version date will be noted but the main policies of the audit will be those that are currently still in place or those that have replaced these deprecated policies. Ability to access the policies will also be noted to ensure that the policies are in place and available to view at any time. In terms of the basic objectives of what will be covered, the protect team will see the organization's policies revolving around access controls, data security, information protection processes and procedures, maintenance, and protective technologies. Anything outside these areas will not be the main focus of this audit.

Checklists

General Provisions

Question	Compliant or Not	Findings	Notes
Does the policy determine who has authority to implement security policy as well as procedures for granting exceptions?	No	IT policy and standard life cycle is missing/not found	This policy is crucial to determine who has authority to implement security policy as well as procedures for granting exceptions.
Is there a way to capture the principal	No	Unavailability of vulnerability threat	These factors are crucial to build a

characteristics of a vulnerability, and produce a numerical score reflecting its severity?		score or metrics.	resilient information security ecosystem
Is there cybersecurity awareness education for all users?	Yes	Continually evolving protection process included with awareness training	N/A
Do the privileged users understand their roles and responsibilities for conducting cyber security related training?	Yes	Responsibilities are managed by the ISM and ISA assigned to the user	N/A
Are access permissions managed? If so, how are they managed?	Yes	Access permissions are managed, thus incorporating the principles of least privilege and separation of duties under the information security considerations	N/A
Are there strict university-wide regulations for misuse or incompliance ?	Yes	Misuse of these computing resources or failure to follow these policies results in penalties and disciplinary action or other legal sanctions.	N/A
Is there a visual representation of the system ?	No	There is no network diagram of the ecosystem to visually determine if high-value/critical systems are separated from high-risk systems.	The absence of procedures to ensure availability is maintained for critical resources such as network bandwidth, CPU, disk utilization, etc is

Is information classified?	Yes	All the Information that is created, collected or stored into three major categories: Restricted, Sensitive and Open	Policies can be adjusted to be more stringent or more lax based on the category of data.

Contingency Planning

Question	Compliant or Not	Findings	Notes
Are periodic backups taken?	Yes	Each Unit will review and update written backup procedures.	N/A
Is data transit protected?	No	No evidence is found	N/A
Are response plans and recovery plans in place?	Yes	Recovery of lost data from offsite backup me is taken and more than one person have authority for each action	N/A
Is there a copy of the organization's risk assessment to ensure vulnerabilities?	No	No evidence is found	N/A
Are devices (laptops, tablets, removable media) used to store confidential data are encrypted?	No	Unknown. No information was given .	N/A

Is risk assessment conducted periodically?	no	Risk assessment is reviewed every 2 years. The recommendation is every year.	N/A
Are integrity checking mechanisms are used to verify software, firmware and information integrity?	Yes	Integrity and validity is verified to prevent from unauthorized access.	N/A
Are regulations regarding the physical operating environment for organizational assets are met?	Yes	A record shall be maintained for all assets designated as crucial.	N/A

Incident Response

Question	Compliant or Not	Findings	Notes
Are system with crucial data labelled separately	No	All System are labelled as crucial and treated as they contain restricted data	N/A
Are authorized users and unauthorized users defined separately?	No	there is no separation of access.	N/A
Are all users informed and trained?	Yes	Reviews of procedures and training is given annually	N/A
Vulnerability scanning are done?	No	No sign of being done.	In the policies we did not find this functionality in place.
Are maintenance of	No	There is no evidence	In the policies there is

logs done properly?		of its being done, no record found.	no description of logged maintenance mentioned
Plan and policies are they getting updated after disaster recovery?	Yes	Contingency plans are implemented and restoration of operation is done.	Recovery plans and policies updates are mentioned.

Physical Security

Question	Compliant or Not	Findings	Notes
Are physical assets being managed and protected based on type of data?	Yes	Standards and guidelines are listed based on whether it is restricted, sensitive, or operational information.	Some data is more important than others and should be properly classified and secured accordingly
Procedures to detect or block unauthorized access?	Yes	There are proper standards and guidelines for access protections	Server rooms are to be locked at all times and restricted by key, code, or electronic card.
Are those responsible for security requirements stated?	Yes	People that are responsible based on campus and type of assets are given	N/A
Are there backup plans in place for emergencies?	Yes	A contingency plan is given which includes a UPS and backup plans for air conditioning failures	Disasters and emergencies should always be accounted for to prevent any unnecessary outages or downtimes
Is there maintenance logs in place ?	Yes	Documentation of all repairs and modifications to physical security related items such as doors, hardwares, and locks are kept for 6	N/A

		years.	
Is there a termination procedure to ensure physical access removal?	No	Procedures for removing physical access when a person leave the organization is not considered.	Dangerous because they can still have access to important data despite leaving
Is every policy up to date?	No	Last updated 2010, some are still pending	N/A
Are end-users access standards defined for each end-user?	Yes/No	Different end-users should not be grouped together and should have more defined access procedures	N/A

Technical Security

Question	Compliant or Not	Findings	Notes
Are there audit logs for tracking?	Yes	Every system to access the University resources is audited.	Only the authorized users are accounted for the activity log.
Is there an automatic logoff?	Yes	When access to sensitive information by an authorized user is left unattended.	For a particular session ID an automatic logoff with a specified time period if unattended can be implemented.
Are risks assessed placed before the system is placed into operation?	Yes	Information systems assessed for the risks are mitigated prior to placing the system into working.	Each information system has a system security plan and vulnerability assessments are checked by keeping the base risks assessed from risk

			assessment.
Are users given online training?	Yes	Users having authorization to the UF resources are given proper online training.	Training and education materials are updated on a regular basis for changing environment.
Logs of input and output information?	No	Input/output information logs information not logged	Particular user information and input/output information must log for future reference
User account scope review	No	User account scope must perform on a regular basis	User account scope must be reviewed, and account scope must be update and invoke/revoke privileges based on that review
Are logical controls in place?	No	VLAN, Logical controls, firewall and network defenses are not in place.	VLAN and firewall must be in place to get complete network defenses.

Information Security and Emails

Question	Compliant or Not	Findings	Notes
Is there a system that rates the importance of data?	Yes	Data is put into three categories, restricted, sensitive, and open and each is dealt with differently.	There is more classified data than others so it is good they are not all handled the same way.
Do they mention the responsibility of data of both users and admins?	Yes	Policy lists both responsibilities for the owners of data and the custodians who handle it.	It is important to clearly state that data protection is also crucial in the admin stage as it is in the user stage.
Is risk assessment required just once or continually?	Yes	Risk assessment of an information system is required every 2 years.	It is important to keep the information system up to date on successful assessments.
Is there a plan setup in case of complete data loss?	Yes	There are procedures for full backup recoveries.	Backups are crucial to ensure you never completely lose data.
Are the backups tested to make sure they are properly working?	Yes	Backups are constantly being tested to ensure they are both up-to-date and reliable.	You want your backups to have the latest information on them.

Are mobile computing devices periodically assessed to ensure they are still encrypted?	No	Mobile computing devices are required to be initially secured when first purchased, but nothing further after.	These devices should be periodically assessed to ensured there is no leak of information.
Is spam mail automatically blocked?	Yes	After the first spam mail from a sender is received, they are notified not to send more and if they do, the sender is added to the blocked list.	Spam mail should not be received because it not only disrupts the work place, it could contain harmful malware.
Are personal emails allowed to be used to conduct business?	Yes	All faculty and staff are required to use ufl.edu to conduct university business.	It is safer to use a provided email that is constantly monitored rather than your own personal email.

References

https://security.ufl.edu/policies/healthcare-information-security-policies/

https://it.ufl.edu/policies/