**University of Florida Health Science Center Information Security Program**

**Audit Document**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Naveen Kumar Reddy Chillakuru**  **nchillakuru@hawk.iit.edu** | **Alejandro Gomez**  **A**  **agomez15@hawk.iit.edu** | **Joshua P. Kazanova**  **A20388849**  **jkazanova@hawk.iit.edu** | **Armita Roohinejad A20344364**  **aroohine@hawk.iit.edu** | **Christopher E. Siegfried**  **csiegfri@hawk.iit.edu** | **Keving A. Zheng**  **Kzheng8@hawk.iit.edu** |  |

Table of Contents

**Scope 3**

**Executive summary 4**

**Finding Facts 5**

**Conclusion and recommendations 7**

**References** **13**

**Scope**

The information used in this report was collected through the review of the relevant documents, covering:

* 1. General Provisions (InfoSec definitions, programs, policies )
  2. Contingency Planning and Incident Response
  3. Physical Controls
  4. Technical Controls (Password, Transmission, Portable Devices, Software)
  5. Contingency Planning and Incident Response
  6. Physical Controls
  7. Technical Controls (Password, Transmission, Portable Devices, Software)

**Executive Summary**

The primary objective of the audit was to assess the efficiency of the existing security measures and practices regarding information security in place at the University of Florida circa 2009, and make the determination if opportunities exist to improve upon current practices.

The objectives of the exercise are listed below:

1. Determine what current practices are in place for Information Security within the organization.
2. Compare 2009 standard with current NIST/NICE and other current best industry practices
3. Once comparison is complete, look for areas of opportunity.
4. Provide remedies or improvements to areas of opportunities.

**Findings of Facts**

Following controls were found for information security standards best practices:

General Provisions

* Contingency Planning
* Incident Response
* Physical Controls
* Technical Controls

**General Provisions:**

* 1. *GP0003.04, General Provisions (Information Security Program Definitions)*
  2. *GP0007.01/GP0007.02, General Provisions (SPICE POLICY and Standard Authority)*
  3. *GP0003.02/GP0003.04/GP0003.06/GP0003.08, (Information Classification, Information Security Program, Information Security Violations Levels, Report Distribution, and Deadlines)*

**Contingency Planning:**

1. *CP0001:* [*Maintaining Information Security During a Disaster*](http://security.ufl.edu/wp-content/uploads/2013/09/CP0001.pdf)
2. *CP0002:* [*Contingency Plan*](http://security.ufl.edu/wp-content/uploads/2013/09/CP0002.pdf)

**Incident Response:**

1. *IR0001 Security Incident Response Team Charter*
2. *IR0001.02 Information Security Incident Classification Matrix*

**Physical Controls:**

1. *Policy PS0001/PS0001.02*
2. *Policy PS0002/PS0002.02/PS0002.04*

**Technical Controls:**

1. *TS0005, User Account and Password Management*
2. *TS0006, Electronic Communications and Data Transmission Policy*
3. *TS0006.02, Electronic Communications and Data Transmission Standard*
4. *TS0010 portable Computing Device Security*
5. *TS0011.01 General Software Security*

**Conclusion and Recommendations**

**General Provisions:**

* 1. Update of the referenced glossary of terms. In addition, IT security administrator should perform glossary updates as needed.

a) Knowledge, Skills, and Abilities (KSAs) are the skills required to perform a job and are generally demonstrated through relevant experience, education, or training. The

Information Security Management Team insures KSAs are defined, comprehension on

behalf of management and non-IT is functional and training is ongoing.

b) A handbook either digital, in print or preferably both, needs to be developed that is more comprehensive than the current article GP0003.04. There are several different information security threats not currently listed. This needs to be addressed immediately. The handbook will be based on the KSA principles found in NICE Cybersecurity Workforce**.**

* 1. Update policy as it applies to information classification, security program definitions, violation levels, and report distribution.

a) Categories and descriptions of duties/responsibilities need to be developed and assigned to appropriate IT support staff as well as non-IT staff.

b) Upon development of an IT infrastructure, proper authorization regarding student records needs to be determined and administered to maintain Federal and State compliance.

* 1. Update of policy regarding information classification, security, and penalties for non-compliance to information security policy. In addition, establish deadlines for information security reporting as it relates to violations and threats.

a) A revision of information security responsibility policy to further define chain of custody as it relates to student and university information. As it exists, it is too vague and does not provide sufficient protection to intellectual property of the university or general information of students and faculty.

b) Established definitions of what constitutes a violation of University information security policy. i.e., Is downloading illegally distributed media on my personal device through a university network grounds for immediate expulsion?

c) The creation of a report, as well as regularly scheduled physical meetings with university decision makers regarding the status of information security practices and incidents. The report must be an audit itself, and have defined goals or benchmarks. It should be thorough in its scope, and include the physical assets of the university that are related to information security**.**

**Contingency Planning:**

* 1. Each unit is responsible for their team. It would improve the procedures In contingency planning if someone outside the unit reviews the plan to get a thorough insight in to the planning.

There should be multiple contingency plans incase both onshore and offshore site is compromised such as an offline backup facility.

Backup should always be available in case one of the unit is unavailable to continue the procedure.

During testing using simulations for the disaster and then trying it on a virtual simulator would be a good idea, since all the plans cannot be testing onsite.

Detailed steps should be written in an order so that there won’t be overlap of plans and recovery in between.

During the testing phase, the time duration should b noted to analyze how long it will take to recover in case of a disaster so as to have a time set to tell the clients about the recovery period.

The clients, stake holders, employees and customers should be made known of the disaster recovery plan as required.

The recovery teams should be well trained in both virtual and onsite scenarios to recover the information based on priority to get the business running.

Strategies should be planned based on the existing disasters that have occurred and plans to recover from such disasters. This should be made well known to the personnel handling the disaster recovery plan and recovery.

There should be plans to check the after math in detail, such as validate the things that are successful and that have failed to be recovered and contingencies for the failed processes and their impact on the organizations.

Documentations should be done while performing the disaster recovery plan, such as

who is executing the plan the stages being followed If they are complained with the planned policy

The personnel involved in the planning

To check if proper milestones have been reached as planned, if not alternate ways to lessen the damage and proceed the business.

* 1. Risk assessment should also include how the clients will be impacted due to the disaster and how their data is being backed up and restored.
  2. Backups to the point of contact

Backup for approval in case of a higher official is not available to approve the procedure during disaster.

Records of personnel involved in the planning, testing and implementation phases.

Risk assessment of each asset and information

Point of contact and their backup information to be made know to personnel to notify about the disaster.

**Incident Response:**

1. Version, Effective Date, Last Review, Next Review of policies are all old, it does not look like they have been looked at for some time.

2. Priorities were not mentioned in the business plan/write up.

3. Theft of data is not addressed in a lengthy and extensive manner, it is only discussed for validation purposes.

4. Resources that support critical functions are not clearly labeled or listed.

NIST policy 3.6.2 Identify Resources that following categories should be stated

1. Time Frames needed
2. Overlap of Areas
3. Analyze Resources Needed
4. Common Resources Used
5. People
6. Processing Capability (e.g., mainframes, personal computers)
7. Computer-Based Services (e.g., telecommunications, world wide web)
8. Data and Applications
9. Physical Infrastructure Documents and Papers (e.g., documentation, blank
10. forms, legal documents)

1. There is not a clear definition of “emergency” or “disaster” mentioned in the beginning policies.

Would recommend that they are more clearly defined and create contingency plans of disasters to define actions during such events, as well as handling of critical resources during these.

2. Version, Effective Date, Last Review, Next Review of policies are all old, it does not look like they have been looked at for some time.

3. There should be a list of smaller and larger contingencies. Less obvious contingencies should be noted as well.

4. CP0002 \_Section 4: Has at least five different people maintaining the latest revision of the plans.This could be too many people and a conflict of roles and assigned jobs, would recommend reducing this number.

Policies IR0001.04 Security Incident Response Team Sequence of Actions, and IR0001.06 Information Security Incident Notification Schedule, are not available for review.

**Physical Controls:**

1. Type of physical access to the facilities itself is not mentioned so I recommend standardizing physical entry into the facility.
2. Install a key card reader at entrances to check who enters the building and ensure that no one unauthorized enters the building.
3. If employees are not trained on the dangers of tailgating, design a program to inform them. (Tailgating is when you follow behind someone who has authorized access into the area without scanning your own card).
4. There are no mentions of video recording devices being in use in these facilities. If there are not security cameras installed, I would recommend installing cameras at all entry and exit points for the building and cameras outside high security rooms, and wherever else deemed necessary.
5. No mentions of standards of security of a door, will there be sensors installed to ensure that the door is actually closed when it should be?

For extra secure areas, use man traps to ensure tailgating does not happen.

2. There is nothing written about how often the list of authorized users is audited. Depending on how well the systems are hooked up into computer systems, there is potential that users who were given access to server rooms for a period of time and have not been removed and this should be checked about once a month or more often to see if people who shouldn’t be on the authorized list should be taken off the list.

1. Access logs are not reviewed often enough, it’s stated that it should be reviewed at least monthly, however I would recommend a hard-set interval of once a week for sensitive information.
2. This does cost money…however…I recommend that all entry and exit points be keycard access only with a key backup and if a key backup IS used, the appropriate people should be alerted that entry was gained into a room without automated electronic record of the event occurring.
3. Doors should not have any sort of window that allows visibility into the room. If possible, apply a solid or opaque film over glass to disallow peering into the room.
4. Only Restrictive/Sensitive server rooms have multi-factor access control, while operational server rooms only require to be locked. Operational doors should also have at least keycard access (more than just a key because keys can be duplicated easily).

**Technical Controls:**

1. Detailed documentation for account distribution along with password confidentiality and user responsibility:
2. Users must not allow another user to use their unique user identification or password.
3. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner
4. If a user believes their user identification has been comprised, they must report that security incident to their manager.
5. Documents that meet requirements for Password Best Practices Policy:
6. Passwords must be a minimum of eight characters in length
7. Passwords must not be words found in a Dictionary
8. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
9. Change of the password periodically (every 90 days).
10. Disabling the user identifier after 90 days of inactivity.
11. Authenticator management:
12. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation.
13. Theft of the devices, be it a computer or storage device, potentially result in a huge breach of information. It is important to have a method of both removing total access to the information as well being able to recover the data lost. In case of theft, there should be a method of remotely destroying the data to prevent any misuse.
14. First party malware that gets distributed without extensive review would be able to infiltrate all systems and carry out whatever.

**References:**

* Technical Access Control AC-1 Access Control Policy and procedures retrieved from<https://nvd.nist.gov/download/800-53/800-53-controls.xml>
* Security Laboratory: Defense in Depth Series retrieved from<https://www.sans.edu/cyber-research/security-laboratory/article/311>
* Data Center Physical security Checklist retrieved from<https://www.sans.org/reading-room/whitepapers/awareness/data-center-physical-security-checklist-416>
* Contingency Planning Guide for Federal Information Systems Retrieved from<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>
* Guidelines for Managing the security of Mobile devices in the enterprise<http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf>
* security considerations in system development life cycle retrieved from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf>