**U08A1 – Access Control, Software Development, and System Maintenance**

**Chris Misch**

School of Business, Technology, and Health Care Administration, Capella University

IT4076: Security Management and Policies

Stuart McCubbrey

June 2023

1. **Overview**

This policy will outline several security policies that need to be created to ensure confidentiality integrity and availability of the High-Class Healthcare systems and data. This policy is an Enterprise Information Security Policy (EISP) outlining what should be included in the developed policies. This policy will help set the direction, scope, and tone for access control, software development, and system maintenance.

* 1. **Purpose**

The purpose of this policy is to outline what needs to be included in each of these defined policies. This policy aims to protect sensitive data ensure the integrity and availability of software systems and comply with applicable privacy regulations and industry best practices.

* 1. **Scope**

The scope of this policy will include access controls, software development, and system maintenance.

1. **Policy**

This policy will be reviewed once a year to ensure it remains current. At the time of review changes or updates may be implemented and a change log will be created and updated for any new changes to this policy. These policies will be tailored to the unique characteristics of High Class Healthcare environment specific to their systems and technologies. They will ensure regulations such as HIPAA and PHI are followed. EISP will align with relevant industry standards, regulations, and best practices. It will be supported by related policies and processes, including but not limited to data privacy, incident response, and risk management.

Training will be provided to all employees, contractors, vendors, and volunteers ensuring full understanding and compliance is maintained.

* 1. **Access Control**

Access Control measures will be implemented to safeguard physical and logical access to the hospital’s systems, data, and resources according to HIPAA 164.308(a)(4) standard. This includes, but is not limited to, the following factors.

1. User authentication and authorization processes
2. Assignment of access rights based on the principle of least privilege.
3. Regular review and revocation of access privileges
4. Physical security controls, such as badge systems and surveillance, and entry.
5. Logging and monitoring of employee access of systems and devices.
6. Periodic reviews of authorized access removing any authorization creep.
7. What information is encryption or hashed and how it is stored.

Access controls are a set of rules that allow a specific group or individual authorized access to a set of actions on a particular set of resources. Access control measures must be added to control access to both physical and logical mechanisms to ensure integrity, confidentiality, and availability of data and systems owned and operated by the hospital system.

Controlling access to the hospital system can use a combination of Mandatory Access Controls (MAC) that are based on a need-to-know authorization. The hospital system can also use Attribute Based Access Control (ABAC) that helps to enforce MAC controls. Identity management implementation will help in securing and defining usernames, passwords, and the use of biometrics.

* 1. **Software Development**

Software development policy activities will adhere to secure coding practices and industry-accepted standards. Factors within the scope of software development security policies will include:

1. Secure software development life cycle (SDLC) practices using NIST Secure Software Development Framework (SSDF)
2. Regular code reviews and vulnerability assessments will be conducted.
3. Implementation of secure coding guidelines and frameworks.
4. Testing and quality assurance procedures to identify and remediate vulnerabilities.
5. Regular updates and patch maintenance
6. Logging of any changes, deletions, or updates to software
7. Regular security training and awareness exercises HIPAA 164.308(a)(5)

For software provided by outside sources, the Service Level Agreement (SLA) should be created to ensure proper security safeguards are in place. The SLA should include security requirements and expectations. There needs to be regular software updates and patching. Logs must be created and maintained to show what has been changed.

Software development security is important in ensuring vendor software and applications are secure and follow High Class HealthCare’s mission statement to ensure safety confidentiality for all patients, employees, individuals, and groups that use their systems. Pentesting must be defined and used to test for known and unknown vulnerabilities of the software.

* 1. **System Maintenance**

System maintenance activities will be conducted to ensure the ongoing security and optimal performance of High-Class Healthcare’s systems. This will include:

1. Regular patch management and updates for operating systems and software
2. Monitoring and logging of system activities including repairs, replacements, or modifications. HIPAA 164.310(a)(2)(iv)
3. Incident response and vulnerability management processes
4. System backups and disaster recovery planning
5. Backup of system data in regular intervals.
6. Disaster recovery will be developed and tested to minimize downtime and ensure quick recovery of hardware, software, and data.

System maintenance policy will cover both physical and logical aspects of High Class HealthCare’s network and systems.

1. **Policy Compliance**

All employees, contractors, vendors, and volunteers must comply with this Operational Management Security Policy, Failure to follow this policy will result in disciplinary action, up to and including termination of employment, services, or contracts.

If any violation of this policy is seen it must be reported to either the IT security department or to the department manager of your assigned department for further investigation or escalation.

1. **Roles and Responsibilities**

Roles and Responsibilities are assigned to current positions within High Class Healthcare.

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| CEO | Oversee and authorize final approval of any changes made to this policy.  Provide leadership and guidance to team members and other stakeholders.  Ensure the development, implementation, and maintenance of the policy. |
| CIO | Oversees the implementation and maintenance of the policies. Ensures compliance with applicable regulations and standards.  Review and update policy every year |
| Network Administrator | Manages the hospital network infrastructure and enforces access controls |
| IT Administrator | Oversees software development processes, including secure coding practices and adherence to software development guidelines |
| Help Desk Supervisor | Provides support and guidance to users, ensuring adherence to access control and security procedures |
| All employees, contractors, vendors, and volunteers | Will comply with all procedures and complete yearly training on policies and procedures. |

1. **Related Standards, Policies, and Processes**

OWASP Top 10

NIST SP800-218 SSDF Secure Software Development Framework Version 1.1

NIST SP800-37

NIST.IR.7874

1. **Definitions and Terms**

CEO – Chief Executive Officer

CIO – Chief Information Officer

C-I-A – Confidential, Integrity, and availability. Refers to ensuring sensitive information is safe, secure, and available to authorized entities only.

1. **Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Summary of Changes | Approval |
| 1.0 | 05/20/2023 | Creation of new policy | Mark Moneybags, CEO |

1. **Resources**

Forsbak, Ø. (2021, November 29). *10 Best Practices for Software Development Security*. Orient

Software. https://www.orientsoftware.com/blog/software-development-security/

*OWASP Top 10:2021*. (n.d.). https://owasp.org/Top10/

Be sure to include:

Didn't see a discussion of how the policy requirements would be communicated to those who need to adhere to it. Best approach would be a combination of methods to communicate the policy: send it to them, make them acknowledge they read it, train them on it, send them reminders to comply.

Notes from ai:

 Application of Contextual Characteristics The policies outlined in this EISP will be tailored to the unique characteristics of the hospital environment, considering factors such as patient privacy, healthcare regulations (e.g., HIPAA), and the specific systems and technologies used within the hospital.

 Policy Compliance All employees, contractors, vendors, and volunteers are required to comply with the provisions of this policy. Noncompliance may result in disciplinary action, including but not limited to, warnings, suspension, termination of employment, or contract termination.

 Policy Noncompliance Procedures and Penalties Procedures for addressing policy noncompliance will be established, including incident reporting mechanisms and investigation processes. Penalties for noncompliance will be commensurate with the severity of the violation and may include disciplinary actions, legal consequences, or termination of employment or contract.

 Related Standards, Policies, and Processes This EISP will align with relevant industry standards, regulations, and best practices. It will be supported by related policies and processes, including but not limited to data privacy, incident response, and risk management.

Ensure that the following information is covered in the policy language proposed:

* Factors within the scope and range of access control and software development and maintenance security policies.
* Roles and responsibilities involved with the various activities included in the policies.
* Application of contextual characteristics specific to the hospital.
* Policy noncompliance procedures and penalties.

When complete, submit your document in the assignment area.

Refer to the Access Control, Software Development, and Maintenance scoring guide for details on how your assignment will be graded.

* Competency 3: Create an appropriate security policy for an organization.
  + Identify most factors appropriate for inclusion in the full range of access control, software development, and maintenance security policies.
  + Identify most roles and responsibilities involved in the various activities included in the full range of access control, software development, and maintenance security policies.
  + Describe most of the specific contextual characteristics that inform the creation of all access control, software development, and maintenance security policies.
  + Describe in detail the procedures and penalties for noncompliance with all access control, software development, and maintenance security policies.
* Competency 5: Communicate effectively.
  + Follow current APA style and formatting guidelines for references and citations and create a clearly written document generally free of grammatical errors.