Hospital IT Security Policy

Prepared by: K. Stewart, A.S., Cybersecurity

Medical Facility, San Francisco, CA

August 20th, 2024

Information Security Policy Overview

This IT security policy establishes guidelines for safeguarding the confidentiality, integrity, and availability of this medical facility's information assets. The aim is to protect patient data, comply with legal and regulatory mandates, including HIPAA, and ensure the organization's operational efficiency. This policy includes all employees, contractors, and third-party entities with access to facility systems and data.

Application Development Security Policy

Objective

To safeguard patient data and system integrity, all application development within the medical facility must adhere to stringent security protocols. This policy mandates secure coding practices, rigorous testing, and controlled access to development environments.

Guidelines

- **Secure Coding:** Prioritize secure coding principles, preventing vulnerabilities like SQL injections, cross-site scripting, and buffer overflows.
- **Security Testing:** Continuous comprehensive security assessments, which include vulnerability scanning, penetration testing, and code reviews; mandatory for all applications.
- **Access Control:** Stringent access controls for development environments, limiting access to authorized personnel only.
- **Documentation:** Detailed records of security requirements, testing results, and remediation actions.

Data Protection and Recovery Policy

Objective

Defend and protect critical data via regular backups and secure storage, mitigating risks from system failures, corruption, or natural disasters.

- **Backup Schedule:** Mandatory regular/daily backups of critical data to off-site secure locations.

- **Data Encryption**: All backup data must be encrypted during transmission and storage to protect against unauthorized access.

- **Retention Policy:** Backups retained for a minimum of six months to enable timely data restoration.

- **Backup Testing:** Regular testing of backup and recovery procedures to validate system functionality and minimize recovery time.

Physical Security

Objective

Install physical security measures to protect the facility's information assets from unauthorized physical access, damage, or theft.

Guidelines

- **Access Control:** Add access control systems restricting entry to sensitive areas to authorized personnel only.

- **Surveillance:** Install and maintain surveillance cameras in critical areas.

- **Secure Storage:** Store sensitive equipment, such as servers and backup media, in a locked, secure area.

- **Visitor Management:** Maintain a visitor log and ensure visitors are escorted by authorized personnel in restricted areas.

Network Device Installation and Configuration

Objective

To defend network devices, including routers, switches, and firewalls. Network devices must be installed and configured securely to protect the facility's network from unauthorized access and threats.

Guidelines

- **Configuration Standards:** Network devices must be configured according to security best practices and updated regularly.
- **Access Control:** Restrict administrative access to network devices to authorized personnel only.
- **Network Segmentation:** Deploy network segmentation to separate sensitive data and systems from general network traffic.
- **Monitoring:** Continuously monitor network devices for suspicious activity and potential security breaches.

Data Handling

Objective

Develop stringent data handling procedures to ensure confidentiality, integrity, and availability (CIA) of sensitive information.

Guidelines

- **Data Classification:** Classify data based on its sensitivity, then apply correct security controls.
- **Encryption:** Encrypt sensitive data during transmission and storage.
- **Access Control:** Limit access to sensitive data to authorized personnel only.
- **Data Disposal:** Ensure sensitive data is securely deleted or destroyed when no longer needed.

Remote Access

Objective

Remote access to the medical facility's information systems must always be controlled and secured to prevent unauthorized access and data breaches.

Guidelines

- **Authentication:** Implement multi-factor authentication for all remote access.
- **Encryption:** Encrypt all remote access connections.
- **Access Control:** Limit remote access to authorized personnel only.
- **Monitoring:** Continuously monitor remote access activity for any suspicious behavior.

Email

Objective

Maintain secure email communications to protect sensitive information from unauthorized access and potential threats.

Guidelines

- **Encryption:** Encrypt emails containing sensitive information.
- **Phishing Protection:** Deploy phishing detection and prevention measures.
- **Access Control:** Restrict email access to authorized personnel only.
- **Retention Policy:** Establish and enforce email retention policies.

Internet and Web Access

Objective

Internet and web access must be controlled and monitored to prevent exposure to malicious websites and unauthorized data transfers.

Guidelines

- **Content Filtering:** Deploy web content filtering to block access to malicious and inappropriate websites.
- **Access Control:** Limit internet access to necessary personnel only.
- **Monitoring:** Continuously monitor internet activity for suspicious behavior.
- **Security Awareness:** Educate employees on safe internet usage practices.

Device Security

Objective

All devices, meaning desktops, laptops, and mobile devices, must be secured to defend against sensitive information being stolen and to prevent any unauthorized access.

Guidelines

- **Device Configuration:** Configure devices according to security best practices.
- **Encryption:** Encrypt sensitive data stored on devices.
- **Access Control:** Implement strong authentication and access controls.
- **Mobile Device Management (MDM):** Use MDM solutions to manage and secure mobile devices.

Process for communicating policy with Stakeholders

Objective

To communicate policy effectively with all stakeholders increasing their understanding of the organization's security posture and maintaining compliance.

Guidelines

- **Training:** Conduct continuous training and awareness programs for all employees.
- **Policy Distribution:** Distribute the security policy to all employees and require acknowledgment of receipt and understanding of the policy.
- **Regular Updates:** Provide regular updates on policy changes and new security threats.
- **Feedback Mechanism:** Establish a feedback mechanism to address questions and concerns related to the security policy.