**Part 1: Review of the Scenario**

ACME Healthcare has faced numerous data breaches, leading to financial losses and reputational damage. With the appointment of a new Chief Information Security Officer (CISO), a comprehensive security audit was conducted, revealing several vulnerabilities across the organization's infrastructure and practices.

**Part 2: Review and Prioritize Audit Findings**

Here's a breakdown of the vulnerabilities identified in ACME Healthcare's security audit, along with their potential impact and likelihood of exploitation:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Vulnerability** | **Potential Impact** | **Likelihood of Exploitation** |
| **Identity and Access Management (IAM)** | Dormant accounts (1) | Unauthorized access to systems and data. | High - Dormant accounts are easy targets for attackers to exploit existing credentials. |
| **IAM** | Unauthorized privileges (2) | Escalated access to sensitive information and systems. | High - Privileged accounts provide extensive control and are attractive targets. |
| **IAM** | Weak password policies (5) & crackable passwords (4) | Breaches of user accounts and access to sensitive data. | High - Weak passwords are easily compromised through brute-force attacks or social engineering. |
| **Data Security** | Unencrypted data on devices (6) & emails (8) | Exposure of sensitive patient information (e.g., PHI) in case of breaches. | High - Unencrypted data is readily accessible to attackers who gain access to devices or emails. |
| **Data Security** | WEP encryption (7) | Weak protection for wireless access points, allowing interception of data. | Medium - WEP is a cracked encryption standard, but exploiting it might require more effort for attackers. |
| **Security Practices** | Unattended devices & unlogged-out sessions (11) | Unauthorized access to systems and potential data exfiltration. | Medium - Opportunistic attackers might exploit unattended devices, but targeted attacks are less likely. |
| **Security Practices** | Inconsistent device updates (12) | Unpatched systems vulnerable to known exploits. | High - Unpatched vulnerabilities are well-documented and readily exploitable. |
| **Security Practices** | Infrequent security log review (9) | Delayed detection of suspicious activity and potential breaches. | High - Unmonitored logs allow attackers to operate undetected for extended periods. |
| **Network Security** | Overly permissive firewall rules (13) | Unnecessary attack vectors for unauthorized access attempts. | Medium - While permissive rules increase the attack surface, targeted exploitation might require additional effort. |
| **Network Security** | Outdated servers (14) | Unpatched vulnerabilities and outdated security features. | High - Outdated servers are prime targets with readily available exploits. |
| **Internal Controls** | Personal use of work devices (10) | Introduction of malware, data leakage, and potential compliance violations. | Medium - The risk depends on the type of personal use. Downloading malware or mishandling data is a concern, but casual use might be lower risk. |
| **Internal Controls** | Intranet web server vulnerability (15) | Unauthorized modification of user information, potentially leading to identity theft. | Medium - The impact depends on the vulnerability specifics. Changing contact information might be less severe than compromising credentials. |

b.     Based on your research, list the top five security audit findings that ACME should address, starting with the greatest vulnerability.

Here are the top 5 security audit findings ACME Healthcare should address, ranked by their potential severity:

1. **Weak Password Management (Findings 4 & 5):** Forty percent of passwords being cracked within 6 hours indicates extremely weak password practices. This, combined with potentially non-standardized password expiration (5), creates a major access point for attackers. Stolen credentials are a common way to breach systems, and the ease of cracking ACME's passwords makes them highly vulnerable.
2. **Unencrypted Data (Findings 6 & 8):** Sensitive files on user devices (6) and emails containing sensitive information being sent unencrypted (8) pose a significant risk. If a device is lost, stolen, or compromised, attackers gain easy access to this sensitive data. This could lead to HIPAA violations, identity theft, and reputational damage.
3. **Dormant Accounts and Unauthorized Privileges (Findings 1 & 2):** Dormant accounts for former employees (1) offer attackers a readily available access point if credentials haven't been disabled. Similarly, user accounts with unauthorized privileges (2) can be exploited to gain access to sensitive information and systems beyond what's necessary for the user's role. Both findings indicate a lack of proper access control, a critical security principle.
4. **Outdated Servers (Finding 14):** Unpatched servers are prime targets for attackers with readily available exploits. Outdated systems are more likely to have vulnerabilities that haven't been addressed, making them much easier to breach.
5. **Infrequent Security Log Review (Finding 9):** Security logs are essential for detecting suspicious activity. If these logs are infrequently reviewed (9), it allows attackers to operate undetected for extended periods, potentially causing significant damage before being discovered.

c.

**Vulnerabilities Ranking Table for ACME Healthcare**

|  |  |  |  |
| --- | --- | --- | --- |
| Rank | Vulnerability | Recommended Policy | Justification |
| 1 | Weak Password Management (Findings 4 & 5) | Implement strong password policies with minimum length, character complexity requirements, and regular mandatory changes.  Educate employees on password hygiene practices (avoid reuse, not sharing passwords). | 40% of passwords being cracked within 6 hours indicates extremely weak password practices. This creates a major access point for attackers. Stolen credentials are a common way to breach systems. |
| 2 | Unencrypted Data (Findings 6 & 8) | Enforce data encryption for all sensitive information at rest and in transit.  Implement device encryption for laptops, desktops, and mobile devices used for work purposes. | Sensitive files on devices and unencrypted emails pose a significant risk of data breaches if a device is compromised. This could lead to HIPAA violations and reputational damage. |
| 3 | Dormant Accounts and Unauthorized Privileges (Findings 1 & 2) | Disable accounts for terminated employees immediately.  Implement least privilege access control, granting users only the permissions necessary for their job function. Regularly review and update user access privileges. | Dormant accounts offer attackers a readily available access point. Unauthorized privileges allow users to access sensitive information beyond their job requirements. Both findings indicate a lack of proper access control. |
| 4 | Outdated Servers (Finding 14) | Implement a system for consistent device updates and vulnerability management.  Prioritize patching critical systems and those containing sensitive data. | Outdated servers are prime targets for attackers with readily available exploits. Unpatched systems are more likely to have vulnerabilities that can be exploited. |
| 5 | Infrequent Security Log Review (Finding 9) | Establish a process for regular and timely review of security logs by qualified personnel.  Implement automated security monitoring tools to detect suspicious activity. | Infrequent log review allows attackers to operate undetected for extended periods. Security logs are essential for identifying and responding to potential security incidents. |

**Part 3: Develop Policy Documents**

1. Choose one vulnerability in the table for which to develop a security policy.

**We picked Unencrypted Data**

b.     Using the [Information Security Policy Templates](https://www.sans.org/information-security-policy/) we developed the following security policy for ACME Healthcare that addresses unencrypted data vulnerability.

**Data Encryption Policy for ACME Healthcare**

**Overview**

This policy establishes the requirements for data encryption at ACME Healthcare to safeguard sensitive information at rest and in transit.

**Purpose**

The primary purpose of this policy is to ensure the confidentiality and protection of sensitive data stored, processed, or transmitted by ACME Healthcare. By encrypting data, we aim to minimize the risk of unauthorized access and potential data breaches.

**Scope**

This policy applies to all employees, contractors, and any other parties who access, process, or store sensitive data on behalf of ACME Healthcare. This includes data on:

* Company-owned devices (laptops, desktops, servers, and removable media)
* Personal devices used for work purposes
* Data transmitted over networks

**Definitions**

* **Sensitive Data:** Any data that could cause harm to the organization or individuals if disclosed or compromised. This includes patient information (protected by HIPAA), financial data, intellectual property, and other confidential information.
* **Encryption:** The process of transforming data into a scrambled format that can only be accessed using a decryption key.

**Policies**

* **Data at Rest:** All sensitive data stored on company-owned devices must be encrypted.
* **Data in Transit:** All sensitive data transmitted over networks must be encrypted using a secure protocol.
* **Device Encryption:** All laptops, desktops, and mobile devices used for work purposes must be configured with full-disk encryption.
* **Encryption Standards:** ACME Healthcare will adopt industry-standard encryption algorithms and key lengths based on the sensitivity of the data.
* **Key Management:** Encryption keys will be securely stored and managed following best practices to prevent unauthorized access.

**Policy Compliance**

Employees are responsible for understanding and complying with this policy. Violations may result in disciplinary action, up to and including termination of employment.

**Related Standard Policies and Processes**

* Password Policy (Link to password policy document)
* Security Incident and Breach Response Policy
* Data Classification Policy

**Review and Updates**

This policy will be reviewed and updated periodically to reflect changes in technology and best practices.

**Training**

ACME Healthcare will provide training to all employees on this policy and data security best practices.

This revised policy incorporates the template you provided, including definitions, an overview of policy compliance, and references to related standard policies such as a password policy.

**Data Encryption Procedure for ACME Healthcare**

**Purpose**

This procedure outlines the step-by-step process for implementing data encryption at ACME Healthcare, as mandated by the Data Encryption Policy.

**Scope**

This procedure applies to all IT staff and employees who are responsible for storing, processing, or transmitting sensitive data on company-owned devices or personal devices used for work purposes.

**Resources**

* Data Classification Policy: [Link to Data Classification Policy]
* IT Help Desk: [Phone number or Email address]
* Encryption Software Information (if applicable): [Link to internal document or knowledge base article with specific software instructions]

**Creating The Procedure**

a.     Create a step-by-step set of instructions that supports your information security policy.

**1. Data Classification:**

* Identify and classify all data according to its sensitivity level based on the Data Classification Policy. This will determine the appropriate encryption requirements. Refer to the Data Classification Policy for details on classification guidelines.
* If you are unsure about the classification level of specific data, contact your supervisor or the IT Security department for clarification.

**2. Data at Rest Encryption:**

**Company-owned devices:**

* **Laptops and Desktops:** IT staff will deploy full-disk encryption on all laptops and desktops. The encryption process will likely happen in the background during your next scheduled maintenance window or upon IT staff request. **No action is required from you at this time.**
* **Servers:** Server encryption will be implemented by IT staff. **No action is required from you at this time.**
* **Removable Media:** You are responsible for encrypting removable media (e.g., USB drives) containing sensitive data before use.
  + **Windows:** Refer to the Encryption Software Information document (link provided in Resources) for specific instructions on using BitLocker Drive Encryption for removable media.
  + **MacOS:** Refer to the Encryption Software Information document (link provided in Resources) for specific instructions on using Disk Utility for removable media encryption.
  + **If you are using a different operating system, contact the IT Help Desk (contact information provided in Resources) for assistance.**

**Personal devices used for work purposes:**

* Employees are encouraged to enable full-disk encryption on personal devices used to access or store work-related data.
* **Windows:** The specific steps to enable encryption will vary depending on your device and operating system version. Refer to Microsoft's documentation for instructions specific to your device: [Insert Link to Microsoft BitLocker Documentation].
* **MacOS:** You can enable disk encryption using Disk Utility. Refer to Apple's Support documentation for instructions: [Insert Link to Apple Disk Utility Encryption Documentation].
* **For other operating systems, consult your device manufacturer's documentation or contact the IT Help Desk (contact information provided in Resources) for assistance.**

**3. Data in Transit Encryption:**

* **Company-issued laptops and desktops:**
  + IT staff will configure these devices to use secure protocols (e.g., TLS, HTTPS) for email, file transfer, and remote access applications. **No action is required from you at this time.**
  + You may observe a lock icon or a green address bar when using secure connections.
* **Secure File Transfer:** IT will implement secure file transfer solutions (e.g., SFTP) for transferring sensitive data across networks. **Contact the IT department for instructions on how to use the secure file transfer solution.**
* **Public Wi-Fi:** Employees are advised to avoid transmitting sensitive data over public Wi-Fi networks. If using public Wi-Fi is unavoidable, use a Virtual Private Network (VPN) connection provided by ACME Healthcare. **Contact the IT Help Desk (contact information provided in Resources) for assistance with configuring a VPN connection.**

**4. Encryption Standards and Key Management:**

* IT will select and implement industry-standard encryption algorithms and key lengths based on the data sensitivity level as defined in the Data Classification Policy. **Users are not required to take any action related to encryption standards or key management.**

**5. Training and Support:**

* IT will provide training to employees on data encryption best practices, including device encryption and secure data transfer methods. **You will be notified of upcoming training sessions.**
* IT will offer support to employees for any technical difficulties related to data encryption. **Contact the IT Help Desk (contact information provided in Resources) for assistance.**

**6. Monitoring and Auditing:**

* IT will regularly monitor and audit data encryption practices to ensure compliance with this policy and identify any potential issues. **Users are not required to take any action related to monitoring and auditing.**

**7. Incident Reporting:**

* Any suspected data breaches or security incidents involving unencrypted data must be reported to the IT Security department immediately. **Report any such incidents to [maximusagbe@gmail.com].**

1. Include all the information that a user would need to properly configure or complete the task in accordance with the security policy. **Additional Information for Users**

* **Performance Impact:** Enabling encryption may cause a slight decrease in device performance. IT has balanced security with performance considerations when selecting encryption solutions.
* **Help and Support:** For any questions or assistance with data encryption procedures, contact the IT Help Desk at [Phone number] or [Email address].
* **Lost Encryption Credentials:** If you lose your encryption credentials (password or recovery key) for a company-owned device, contact the IT Help Desk immediately. They will be able to assist you with regaining access to the device following a secure verification process.
* **Unauthorized Software:** Do not install any third-party encryption software on company-owned devices without prior approval from the IT department. Unauthorized software may not meet security standards or cause compatibility issues.