Here’s a detailed analysis of **PCI-DSS Requirement 3** (Protecting Stored Data), which includes practical implementation steps, examples of documents (policies and procedures), and recommendations for the employees involved in the process.

PCI-DSS Requirement 3: Protecting Stored Data

Goal: Ensure that stored **Cardholder Data (CHD)**, such as **Primary Account Numbers (PANs)**, is protected by implementing strong encryption, masking, and key management practices. It also ensures that sensitive authentication data is not stored.

Key Sub-Requirements of Requirement 3:

1. Limiting CHD Storage and Retention to Essential (3.1)

- **Description**: Store only the necessary cardholder data (CHD) and limit how long it is retained.
- **Action Steps**:
    - Establish a **Data Retention Policy** that clearly states the purpose of retaining CHD and how long it should be kept.
    - Define procedures for securely **disposing of CHD**, including shredding printed materials and securely wiping digital files.

Example:

A retail company retains CHD only for payment processing purposes. After 90 days, the data is automatically deleted from the system, and printed records are shredded.

---

2. Not Storing Sensitive Authentication Data (SAD) (3.2)

- **Description**: Sensitive data such as **CVV codes**, **PINs**, or **magnetic track** information should never be stored after authorization.
- **Action Steps**:
    - Ensure no system, database, or application retains SAD.
    - Implement **auditing** to ensure no SAD is being stored unintentionally.

Example:

The company's payment processing system is designed to discard **CVV codes** after the authorization is complete. Regular audits ensure no SAD is stored anywhere in the system.

---

3. Masking Stored PANs (First 6 + Last 4 Digits) (3.3)

- **Description**: Cardholder data should be masked when displayed to users, showing only the first six and last four digits of the PAN.
- **Action Steps**:
    - Implement **role-based access** to ensure only authorized users can view full PANs.

- Ensure all employees can only view masked PANs unless authorized for full access.

Example:

In a customer service portal, only authorized managers can see the full PAN. All other employees see only the masked PAN (e.g., 1234 56XX XXXX 7890).

---

4. Rendering PAN Unreadable on All Communication Channels (3.4)

- **Description**: PANs must be rendered unreadable during transmission over public networks using encryption, masking, or tokenization.
- **Action Steps**:
  - Ensure strong encryption (e.g., **AES-256**) is used for all communication channels that transmit PANs.
  - Implement **SSL/TLS** protocols for all network communications involving CHD.

Example:

An online retailer uses **AES-256 encryption** and SSL/TLS to ensure that PANs are unreadable during payment processing and are not stored in plaintext anywhere in the system.

---

5. Procedures for Encryption Key Protection (3.5)

- **Description**: Encryption keys must be securely stored and managed to prevent unauthorized access.
- **Action Steps**:
  - Limit access to encryption keys to authorized personnel only.
  - Store encryption keys in **hardware security modules (HSMs)** or secure vaults.

Example:

The encryption keys used to secure CHD are stored in a **dedicated HSM** that only authorized security personnel can access. Regular audits ensure that the encryption keys are protected.

---

6. Procedures for Encryption Key Management (3.6)

- **Description**: Establish procedures for **key generation**, **storage**, **distribution**, and **rotation**.
- **Action Steps**:
  - Define the **cryptoperiod** for each encryption key (e.g., how long a key is valid before it must be rotated).
  - Use **dual control** and **split knowledge** for key management to prevent unauthorized use.

Example:

The company’s cryptoperiod for each encryption key is set to one year. After this period, keys are rotated, and the old keys are securely destroyed. **Split knowledge** ensures no single employee has full access to the keys.

---

7. Documenting and Enforcing Policies and Procedures (3.7)

- **Description**: Ensure that all encryption and security procedures are documented, enforced, and regularly reviewed.
- **Action Steps**:
    - Create and distribute security policies covering **encryption, key management, CHD storage, and data retention**.
    - Train all employees on these policies, especially those with access to sensitive data.

Example:

The company maintains a **Security Policy Manual** that outlines the procedures for protecting CHD and encryption key management. All employees receive regular training to stay updated on security best practices.

Policies and Procedures Documents Examples

Here are **three key documents** that a company must prepare and maintain:

1. Data Retention Policy:

- **Purpose**: To define the duration and purpose for which CHD is retained.
- **Key Elements**:
    - Duration of CHD storage (e.g., 90 days after processing).
    - Secure disposal methods (e.g., shredding, wiping hard drives).
    - Quarterly review of the data retention process.

Download Sample: Data Retention Policy Example

---

2. Encryption Key Management Policy:

- **Purpose**: To ensure that encryption keys are securely managed throughout their lifecycle.
- **Key Elements**:
    - Procedures for **key generation**, **distribution**, and **rotation**.
    - **Cryptoperiods** and guidelines for key expiration and destruction.
    - Dual control and split knowledge for key management.

Download Sample: Encryption Key Management Policy Example

---

3. CHD Masking and Access Control Policy:

- **Purpose**: To define how PANs should be masked and who can access full PANs.
- **Key Elements**:
    - **Masking rules** (e.g., first 6 and last 4 digits visible).
    - **Role-based access control** to ensure that only authorized personnel can view full PANs.

- Procedures for reviewing access permissions.

Download Sample: CHD Masking and Access Control Policy Example

---

Implementation Steps for Each Employee Role

1. DevOps Team

- **Responsibilities**:
  - Apply encryption protocols to all systems storing or transmitting CHD.
  - Ensure encryption keys are stored in secure environments (e.g., HSMs).
- **Tools to Use**:
  - **SSL/TLS** for secure communication.
  - **Automated Encryption Management** tools for key rotation and distribution.

2. System Administrators

- **Responsibilities**:
  - Enforce masking policies for PANs and ensure strong encryption for stored CHD.
  - Regularly audit all systems to ensure compliance with encryption and key management policies.
- **Tools to Use**:
  - **Disk Encryption Tools** (e.g., BitLocker, LUKS).
  - **Key Management Systems** for managing and auditing encryption keys.

3. IT Security Team

- **Responsibilities**:
  - Create, update, and enforce security policies covering encryption and CHD protection.
  - Conduct regular audits and risk assessments to ensure the company is PCI-DSS compliant.
- **Tools to Use**:
  - **Security Information and Event Management (SIEM)** tools for real-time monitoring.
  - **Vulnerability scanners** to identify misconfigurations in encryption or access controls.

4. Project Managers

- **Responsibilities**:
  - Ensure all encryption and CHD storage requirements are met in project timelines.
  - Allocate resources for training and tools needed to comply with PCI-DSS Requirement 3.
- **Tools to Use**:
  - **Project Management Tools** (e.g., Jira, Asana) for tracking compliance-related tasks.

By following the best practices outlined in **PCI-DSS Requirement 3**, companies can ensure that **cardholder data** remains secure and compliant with industry standards.

****
Policies example:

1. Data Retention Policy

Purpose:

The purpose of this policy is to define the requirements for retaining cardholder data (CHD) and to ensure its secure disposal when no longer needed.

Policy Details:

1. **Retention Period:**
    - CHD should be retained only for the period necessary to meet legal, regulatory, and business requirements.
    - The maximum retention period for CHD is **90 days** after the completion of a transaction.
    - After the retention period, all CHD must be securely deleted or destroyed.
2. **Secure Disposal Methods:**
    - **Printed Materials:**
        - Shred all physical documents containing CHD using cross-cut shredders.
        - Alternatively, use professional document destruction services.
    - **Electronic Data:**
        - Securely erase electronic files containing CHD using industry-standard data wiping tools that ensure data cannot be recovered.
        - Overwrite data at least three times or use cryptographic erasure methods.
3. **Quarterly Review:**
    - The data retention and disposal procedures will be reviewed quarterly by the IT Security Team.
    - Any discrepancies or non-compliance issues must be addressed immediately.

Responsibilities:

- **IT Security Team:** Oversee the implementation of this policy and conduct regular reviews.
- **All Employees:** Comply with data retention limits and follow disposal procedures.

---

2. Encryption Key Management Policy

Purpose:

To ensure the secure generation, distribution, storage, rotation, and destruction of encryption keys used for protecting cardholder data.

Policy Details:

1. **Key Generation:**
    - Encryption keys must be generated using strong cryptographic algorithms compliant with industry standards (e.g., AES-256).
    - Use secure key generation tools or hardware security modules (HSMs).
2. **Key Storage:**
    - Store encryption keys securely in HSMs or encrypted key vaults.
    - Limit access to encryption keys to authorized personnel only.
    - Do not store encryption keys in the same location as the encrypted data.
3. **Key Distribution:**
    - Distribute encryption keys securely using encrypted channels.
    - Implement dual control procedures where two authorized individuals are required to access or distribute keys.
4. **Key Rotation (Cryptoperiod):**
    - Define a cryptoperiod for each key, not exceeding **one year**.
    - Rotate keys regularly and immediately if a key is suspected to be compromised.
5. **Key Destruction:**
    - Securely destroy obsolete or compromised keys using methods that prevent recovery.
    - Document the destruction process and have it witnessed by authorized personnel.
6. **Access Control and Monitoring:**
    - Implement role-based access control (RBAC) to restrict key access.
    - Maintain logs of all key management activities for auditing purposes.
7. **Incident Response:**
    - In the event of a key compromise, immediately enact incident response procedures.
    - Notify all relevant stakeholders and replace affected keys.

Responsibilities:

- **IT Security Team:** Manage key lifecycle processes and ensure compliance.
- **Authorized Personnel:** Follow procedures for key handling and report any security incidents.

---

3. CHD Masking and Access Control Policy

Purpose:

To define the masking of Primary Account Numbers (PANs) and establish strict access controls to protect cardholder data.

Policy Details:

1. **PAN Masking:**
    - When displayed, PANs must be masked to show only the **first six** and **last four digits** (e.g., 1234 56XX XXXX 7890).

    - Full PANs must not be visible on screens, reports, or printed documents unless absolutely necessary and authorized.
2. **Access Control:**
    - Implement role-based access control (RBAC) to restrict access to systems displaying full PANs.
    - Only employees with a legitimate business need may access unmasked PANs.
    - Access rights must be approved by management and reviewed quarterly.
3. **Logging and Monitoring:**
    - Log all access to systems where full PANs can be viewed.
    - Monitor logs regularly to detect unauthorized access or suspicious activities.
4. **Employee Training:**
    - Train employees on the importance of CHD protection and proper handling procedures.
    - Provide regular updates on security policies and best practices.
5. **Incident Response:**
    - Immediately report any unauthorized access or disclosure of PANs to the IT Security Team.
    - Follow the incident response plan to mitigate risks and notify affected parties if necessary.

Responsibilities:

- **IT Security Team:** Implement and enforce masking and access control measures.
- **Managers:** Approve access requests and ensure their team complies with policies.
- **Employees:** Adhere to access controls and report any security concerns.

Note: Please ensure that these policies are reviewed by your legal and compliance teams to align with your company's specific requirements and local regulations. Customize the policies as needed to fit your organizational context