Summary of PCI-DSS Requirement 4: Protect Transmitted Data

Goal: Protect **cardholder data (CHD)** when it is transmitted across open or public networks. This requirement emphasizes using **strong encryption** and securing all transmission channels to prevent unauthorized access to sensitive information like the **Primary Account Number (PAN)**.

Key Sub-Requirements of Requirement 4:

1. Use Strong Encryption and Security (4.1)

- **Description**: Ensure all transmissions of **CHD** use **strong encryption protocols** to protect the data from being intercepted or tampered with.
- **Action Steps**:
    - Use **strong encryption** protocols (e.g., **TLS 1.2** or higher) for all transmissions involving CHD.
    - Avoid using deprecated or weak encryption protocols like **SSL** or **WEP** for wireless networks.
    - Ensure only **trusted keys** and **certificates** are used.

Example:

When transmitting customer payment details over the internet, an online store uses **AES-256 encryption** over a **TLS 1.2** connection. This ensures that cardholder data is secure in transit and cannot be intercepted by attackers.

---

2. Never Send Unprotected PANs in IM (4.2)

- **Description**: PANs must never be sent unprotected over **instant messaging (IM)** systems or **email**. If they must be transmitted through these channels, they should be encrypted and masked.
- **Action Steps**:
    - Avoid sending PANs through **IM** or **email** unless absolutely necessary.
    - If PANs must be sent, ensure they are **encrypted** and **masked** (e.g., displaying only the first 6 and last 4 digits).
    - Establish a policy to define the circumstances where PANs can be sent and how encryption should be applied.

Example:

A financial institution needs to send payment details via email for reconciliation purposes. Before sending the email, they ensure the PAN is masked (e.g., **1234 56XX XXXX 7890**) and the email is encrypted with **PGP encryption**.

---

3. Document and Enforce Policies and Procedures (4.3)

- **Description**: Document all policies related to the transmission of CHD and ensure that these policies are enforced across the organization.

- **Action Steps**:
  - Create clear policies that define how CHD is transmitted securely across public and internal networks.
  - Ensure employees understand the policies and are regularly trained.
  - Regularly audit and enforce these policies to ensure compliance.

Example:

An e-commerce company maintains a **data transmission policy** that requires all employees to use secure email gateways with encryption for transmitting any customer data. The policy is reviewed annually, and all employees are trained in its use.

Implementation Steps for Each Employee Role

1. DevOps Team

- **Responsibilities**:
  - Ensure all transmissions of CHD use **TLS 1.2+** or higher.
  - Configure **VPN** or **secure communication channels** for internal network communication.
- **Tools to Use**:
  - **SSL/TLS certificates** for encryption.
  - **VPNs** for internal data transmission.
- **Documentation**:
  - Provide documentation on the encryption standards used for each transmission channel (e.g., email, web traffic, internal API calls).

2. System Administrators

- **Responsibilities**:
  - Ensure all email servers and messaging platforms used in the company encrypt communications.
  - Monitor communication channels to prevent any unprotected PAN transmissions.
- **Tools to Use**:
  - **Encrypted email systems** (e.g., PGP, S/MIME).
  - **Data Loss Prevention (DLP) tools** to monitor and block unprotected PAN transmissions.

3. IT Security Team

- **Responsibilities**:
  - Create and enforce the policies related to CHD transmission.
  - Conduct regular audits of network traffic to ensure compliance with encryption policies.
- **Tools to Use**:
  - **SIEM (Security Information and Event Management)** tools to monitor for potential security incidents.
  - **Penetration testing tools** to ensure network encryption is secure.

4. Project Managers

- **Responsibilities**:
  - Ensure that security requirements for data transmission are included in project planning.
  - Allocate resources for implementing and maintaining secure transmission protocols.
- **Tools to Use**:
  - **Project management tools** (e.g., Jira) for tracking compliance-related tasks.
  - **Compliance checklists** to ensure that Requirement 4 is being met.

Policies and Procedures Documents Examples

Here are examples of documents that must be created for compliance with Requirement 4:

1. Secure Data Transmission Policy

- **Purpose**: To define how CHD must be transmitted across networks to ensure compliance with PCI-DSS.
- **Key Elements**:
  - Protocols to be used (e.g., **TLS 1.2+**, **AES-256 encryption**).
  - Rules for masking PANs when sent via email or IM.
  - Guidelines for using secure email and VPNs.

Download Sample: Secure Data Transmission Policy Example

---

2. Encryption Policy for Email and Messaging Systems

- **Purpose**: To ensure that all sensitive data, including PANs, sent via email or messaging systems, is encrypted and masked.
- **Key Elements**:
  - Instructions for encrypting emails with **PGP** or **S/MIME**.
  - Rules for masking PANs in communications.
  - Procedures for reviewing and updating encryption keys.

Download Sample: Email Encryption Policy Example

---

3. VPN Usage Policy

- **Purpose**: To define the use of VPNs for secure internal data transmission.
- **Key Elements**:
  - Guidelines for accessing internal resources over VPN.
  - Rules for encrypting traffic within the corporate network.
  - Access control for VPN users.

Download Sample: VPN Usage Policy Example

Conclusion and Best Practices for the Company

1. **Use Strong Encryption**: All transmissions of CHD over public networks must use **strong encryption protocols** such as **TLS 1.2+**.
2. **Avoid Sending PANs via IM/Email**: If unavoidable, ensure PANs are encrypted and masked.
3. **Document and Enforce Policies**: Ensure all policies related to secure transmission are documented and regularly reviewed.
4. **Employee Training**: Regularly train employees on secure data transmission practices, and ensure they understand the importance of compliance with PCI-DSS.

By following these guidelines and using the provided policies, companies can ensure secure transmission of cardholder data and maintain PCI-DSS compliance.

1. Secure Data Transmission Policy

Purpose: This policy aims to ensure that cardholder data (CHD) is securely transmitted over public and internal networks by implementing strong encryption and masking.

Policy Details:

1. **Encryption Protocols**:
   - All transmission of CHD must use **TLS 1.2** or higher.
   - For internal communications, **VPNs** or encrypted tunnels must be used.
2. **Masking PANs**:
   - When sending PANs via email or messaging systems, they must be masked (showing only the first 6 and last 4 digits).
   - If PANs are sent, emails or messages must be encrypted using **PGP** or **S/MIME**.
3. **Communication Channels**:
   - Secure communication channels such as **VPNs**, encrypted email systems, and secure FTP must be used for transmitting CHD.
   - Unprotected methods like instant messaging or plaintext email are prohibited.

---

2. Email Encryption Policy

Purpose: To define the process for encrypting emails and messaging systems that involve the transmission of sensitive data, including cardholder data (CHD).

Policy Details:

1. **Encryption Methods**:
   - All emails containing CHD must be encrypted using **PGP** or **S/MIME**.
   - No email with unmasked PANs should be sent without encryption.
2. **Masking PANs**:

    - PANs should be masked (first 6 and last 4 digits) when transmitted through email, even when encrypted.
3. **Key Management**:
    - Encryption keys used for email communication must be rotated annually or sooner if compromised.
    - Only authorized personnel should have access to encryption keys.

---

3. VPN Usage Policy

Purpose: This policy defines the use of VPNs for secure access to internal resources and cardholder data (CHD) within the corporate network.

Policy Details:

1. **VPN Usage**:
    - All remote access to internal resources that involve CHD must be done over **VPN**.
    - VPN connections must use strong encryption protocols such as **AES-256**.
2. **Access Control**:
    - VPN access must be limited to authorized personnel with role-based access control.
    - VPN access logs must be maintained and reviewed regularly to detect unauthorized access.
3. **Monitoring and Maintenance**:
    - Regular monitoring of VPN connections and logs must be done by the IT Security team.
    - All VPN configurations must be reviewed annually for security compliance.