Summary of PCI-DSS Requirement 5: Prevent Malware

Goal: Protect all systems that handle **Cardholder Data (CHD)** by ensuring that appropriate anti-virus (AV) software is installed, regularly updated, and cannot be disabled by individual users. Regular scanning and logging should also be enforced to detect malware.

Key Sub-Requirements of Requirement 5

1. Install Anti-Virus Software on Commonly Affected Systems (5.1)

- **Description**: All systems that are vulnerable to malware attacks, regardless of the operating system, must have AV software installed.
- **Action Steps**:
  - Install **anti-virus software** on commonly accessed systems such as **Windows**, **macOS**, and **Linux** servers or desktops that deal with CHD.
  - Regularly review which systems are "commonly affected" and ensure they have proper AV protection.

Example:

A company installs **anti-virus software** on all its workstations and servers that handle customer transactions, including the internal network where customer data is processed. The AV runs in the background and scans regularly for potential threats.

---

2. Frequent Updating, Scanning, and Logging (5.2)

- **Description**: Anti-virus software must be **frequently updated**, scan periodically, and log its activity. Logs should be retained for auditing.
- **Action Steps**:
  - Update **AV software** regularly to protect against new threats.
  - Schedule periodic scans on all systems, and ensure that all logs are **retained** as per company policy (e.g., 90 days).
  - Review logs periodically to detect any suspicious activity.

Example:

A financial company sets its AV software to automatically update definitions and run scans on all machines every **24 hours**. The results are logged, and logs are kept for **6 months** for review in case of a security incident.

---

3. Anti-Virus Software Cannot Be Disabled by Users (5.3)

- **Description**: Individual users must not be able to disable the AV software unless approved by management.
- **Action Steps**:
  - Implement **policies** and **user controls** to prevent users from disabling AV software.

        - Allow temporary exceptions only if there is a valid business reason and management approval.

Example:

An employee needs to disable AV software temporarily for performance reasons during a CPU-intensive operation. The employee submits a request to the IT security team, which approves the action for a limited time with proper logging.

---

4. Document and Enforce Policies and Procedures (5.4)

- **Description**: All policies and procedures related to AV software, scanning, and updates should be documented and enforced.
- **Action Steps**:
    - Document the company’s AV software policies and procedures, ensuring all employees are aware of them.
    - Conduct **training** for employees on the importance of AV software and how it protects the company from malware attacks.
    - Regularly review policies to ensure they are up to date.

Example:

The company maintains a **Malware Protection Policy** that details the responsibilities of each department to ensure AV software is installed, updated, and monitored. The policy is reviewed annually and updated as necessary.

Roles and Responsibilities

1. IT Security Team

- **Responsibilities**:
    - Install, configure, and maintain AV software on all systems.
    - Ensure all systems are scanned regularly, and logs are retained.
- **Tools to Use**:
    - **Anti-virus management console** for remote updates and monitoring.
    - **Log aggregation tools** to store and review AV activity.

2. System Administrators

- **Responsibilities**:
    - Ensure that all machines have AV software and prevent users from disabling it.
    - Monitor the systems for any unauthorized changes in AV configuration.
- **Tools to Use**:
    - **Configuration Management Tools** to prevent unauthorized modifications.
    - **Alerts** for systems that are not running AV software.

3. Project Managers

- **Responsibilities**:

    - Ensure that new systems or software introduced in the company are compliant with AV requirements.
    - Allocate resources for AV software licenses and monitoring tools.
- **Tools to Use**:
    - **Project management software** (e.g., Jira, Trello) to track compliance tasks.

4. Employees (End-Users)

- **Responsibilities**:
    - Do not attempt to disable or interfere with AV software.
    - Report any malware alerts to the IT department immediately.
- **Training**:
    - Employees should be trained regularly on how malware can impact company systems and the importance of keeping AV software active.

Sample Policy Documents

Here are examples of documents that must be created for compliance with Requirement 5:

1. Malware Protection Policy

- **Purpose**: To define how malware protection is implemented and maintained across all systems.
- **Key Elements**:
    - Installation and updating of AV software.
    - Procedures for scanning and logging malware-related activities.
    - Policies preventing users from disabling AV software.

Download Sample: Malware Protection Policy Example*

---

2. Anti-Virus Software Usage Policy

- **Purpose**: To outline the usage and restrictions regarding anti-virus software on all systems that handle CHD.
- **Key Elements**:
    - Requirements for updating AV software.
    - Guidelines for scanning frequency and log retention.
    - Steps for handling requests to disable AV temporarily.

Download Sample: Anti-Virus Software Usage Policy Example*

By adhering to these sub-requirements and documenting the necessary procedures, companies can ensure that they maintain a strong defense against malware attacks and comply with **PCI-DSS Requirement 5**.

1. Malware Protection Policy*

Purpose:
To define how malware protection is implemented and maintained across all systems to ensure compliance with PCI-DSS and secure the environment from malware-related threats.

Policy Details:

1. **Installation and Updates**:
   - All systems must have up-to-date anti-virus (AV) software installed, configured to scan and detect malware threats.
   - AV software must automatically update its virus definitions and be capable of removing or quarantining detected malware.
2. **Scanning and Logging**:
   - Schedule regular system-wide scans, ensuring all files, including those stored and transmitted, are scanned.
   - Logging must be enabled to record scan results and potential threats. Logs should be reviewed regularly by the IT Security Team.
3. **Policy for Disabling AV Software**:
   - AV software cannot be disabled by any user without prior approval from the IT department. Exceptions must be documented, with time limits for disabling.

---

2. Anti-Virus Software Usage Policy*

Purpose:
To outline the requirements and usage guidelines for anti-virus software on all systems that handle sensitive cardholder data (CHD) to ensure compliance with PCI-DSS.

Policy Details:

1. **Updating Anti-Virus Software**:
   - Anti-virus software must be kept up-to-date on all systems handling CHD.
   - Virus definitions must be updated automatically to ensure protection from the latest threats.
2. **Scanning Frequency and Log Retention**:
   - Full scans of systems must occur at least once per week, with incremental scans occurring daily.
   - All scans and AV activities should be logged. Logs must be retained for at least 90 days.
3. **Handling Requests to Disable Anti-Virus Software**:
   - Any request to disable anti-virus software must be submitted to and approved by the IT Security Team.
   - Temporary disabling should only be permitted for specific business purposes and must be tracked.