ChecklistGuro

Credit Card Terminal Security Checklist (Quarterly) - PCI Compliance

Physical Security of Terminals

Ensures terminals are physically protected from theft, tampering, and unauthorized access.

Terminal Location Security Assessment

- □ Secure – Visible and Protected
- □ Potentially Vulnerable – Requires Mitigation
- □ Unsecure – Immediate Action Required

Physical Security Controls in Place (Check all that apply)

- □ Cable Locks/Security Devices
- □ Secure Enclosure/Mount
- □ Visible to Staff
- □ Away from Public Access
- □ None

Number of Terminals Locked/Secured

Enter a number...

Notes on Physical Security Observations

Write something...

Terminal Location (GPS Coordinates - If Applicable)

Set My Current Location

Terminal Mobility Risk Assessment

□ Low – Rarely Moved

□ Medium – Occasionally Moved within a controlled area

□ High – Frequently Moved and Unsecured

Software and Firmware Updates

Confirms terminals are running the latest approved software and firmware versions.

Last Firmware Update Date

Enter date...

Firmware Version Installed

Enter a number...

Update Source Verification

- ☐ Vendor Website
- ☐ Payment Processor
- ☐ Other (Specify in Long Text)

If 'Other' selected above, please specify update source:

Write something...

Software Version Installed

Upload Screenshot of Terminal Software Version (Optional)

Upload File

Is Automated Update Enabled?

- ☐ Yes
- ☐ No

If automated updates are disabled, describe the manual update process:

Write something...

Network Security & Connectivity

Verifies secure network connections and configurations for terminal communication.

Terminal Connection Type

□ Direct Ethernet

□ Wireless (Wi-Fi)

□ Dial/Modem

□ Other (Specify in Long Text)

Wireless Encryption Protocol (if applicable)

□ WPA2

□ WPA3

□ WEP (Not Recommended - Upgrade Immediately)

□ Not Applicable (Direct Ethernet)

Firewall Rule Review Frequency (in days)

Enter a number...

Description of any VPN configurations (if applicable)

Write something...

Network Segmentation

□ Terminals are on a segmented network

□ Terminals are on the main business network

Last Network Scan Date

Enter date...

Details of any network intrusion detection/prevention systems (IDS/IPS) in place

Write something...

Public Wi-Fi Usage

□ Terminals are never connected to public Wi-Fi

□ Terminals are connected to public Wi-Fi (Not Recommended - Requires Specific Measures)

Merchant Account & Configuration

Validates correct merchant account settings, PIN truncation settings, and other critical configurations.

Confirm Merchant Category Code (MCC) is Accurate

□ Yes

□ No

□ N/A

Confirm Maximum Transaction Limit (if applicable)

Enter a number...

PIN Truncation Enabled?

□ Yes, Truncated

□ No, Not Required

□ N/A - No PIN Entry

Verify Correct MID(s) are Active

□ Yes, all correct

□ No, Requires Investigation

□ N/A

Document Any Merchant Account Configuration Changes

Write something...

Is Address Verification System (AVS) Enabled?

□ Yes

□ No

□ N/A

Employee Training & Awareness

Confirms employee training covers secure card handling and terminal operation procedures.

Which of the following topics were covered in the employee's card terminal security training?

□ Cardholder Data Security (CDS) Best Practices

□ Phishing and Social Engineering Awareness

□ Physical Security of Terminals

□ Reporting Suspicious Activity

□ Proper Card Handling Procedures

□ Secure Password Management

What is the employee's understanding of the importance of never leaving a terminal unattended?

□ Fully Understands

□ Somewhat Understands

□ Needs Further Training

Briefly describe the employee’s understanding of how to identify and respond to potential skimming devices.

Write something...

Number of employees who received card terminal security training this quarter.

Enter a number...

Date of employee's last card terminal security training.

Enter date...

Does the employee understand the policy on verifying cardholder identification?

□ Yes

□ No

□ Unsure

Data Encryption & Tokenization

Reviews encryption methods used and verifies correct implementation of tokenization (if applicable).

Encryption Method Used (e.g., EMV, SSL/TLS, HCE)

□ EMV Chip and PIN

□ SSL/TLS

□ HCE (Host Card Emulation)

□ Other (Specify in Long Text)

Encryption Key Rotation Frequency (in days)

Enter a number...

Is Encryption at Rest Implemented?

□ Yes

□ No

□ N/A (Not Applicable)

Description of encryption key management practices. (Who manages, storage, rotation process)

Write something...

Is Tokenization Used for Sensitive Cardholder Data?

□ Yes
□ No
□ N/A (Not Applicable)

Tokenization Implementation Documentation (e.g., vendor agreements, configuration details)

Upload File

Describe how cardholder data is protected during transmission (e.g., Transport Layer Security (TLS) version)

Write something...

Terminal Configuration & Settings

Covers specific terminal settings and configurations that impact security.

Terminal Timeout (Idle Time) in Minutes

Enter a number...

PIN Truncation Enabled?

- □ Yes
- □ No
- □ Not Applicable

Dual-Swipe/Chip Enabled?

- □ Yes
- □ No
- □ Not Applicable

ECR Integration Method (if applicable)

- □ Direct Integration
- □ Through Payment Gateway
- □ Manual Entry
- □ Not Applicable

Maximum Transaction Amount Limit (if applicable)

Enter a number...

Cardholder Verification Method (CVM) List Configuration

- □ Online CVM
- □ Offline CVM
- □ As Per Processor Guidelines

Notes/Comments Regarding Terminal Settings

Write something...

Incident Response & Reporting

Ensures procedures are in place for reporting and responding to security incidents.

Date of Last Incident Response Drill

Enter date...

Briefly describe the incident response plan for card terminal compromise.

Write something...

Who is responsible for initial incident reporting?

- □ Store Manager
- □ Designated Security Personnel
- □ IT Department
- □ Payment Processor Contact

Estimated Time to Recover from a Compromised Terminal (in hours)

Enter a number...

Which reporting entities are included in the incident response plan?

□ Payment Processor

□ Acquirer

□ PCI Security Council

□ Internal Security Team

□ Law Enforcement (if applicable)

Describe the process for securing physical evidence following a suspected breach.

Write something...

Method of documentation of incident details (e.g. paper log, electronic system)

□ Paper Log

□ Electronic System

□ Both