PIN HANDLING AND POI DEVICE SECURITY

Last Updated 12 June 2025

This document outlines the mandatory procedures for all personnel involved in handling cardholder data and operating Point of Interaction (POI) devices to ensure compliance with PCI PIN Security Requirements and PCI DSS (Payment Card Industry Data Security Standard). Adherence to these procedures is critical for maintaining a secure payment environment and protecting sensitive cardholder information.

DEFINITIONS

- **PERSONNEL:** Any individual employed by or otherwise engaged with the organisation (e.g., full-time, part-time, temporary staff, contractors, or third-party service providers) who may interact with cardholder data or Point of Interaction (POI) devices.
- **CARDHOLDER:** The consumer or individual to whom a payment card (e.g., credit card, debit card) has been issued.
- **PERSONAL IDENTIFICATION NUMBER (PIN):** A numeric password used by a cardholder to authenticate themselves to an electronic payment system when using a debit or credit card.
- **POINT OF INTERACTION (POI) DEVICE:** A terminal or device used to capture cardholder payment information, including magnetic stripe data, EMV chip data, or PIN entry. These are commonly known as POS terminals or card readers/card machines.
- **TAMPERING:** Any unauthorized modification, alteration, or substitution of a POI device, its components, or its software, intended to compromise its security or functionality (e.g., to capture cardholder data or PINs).

1. CARDHOLDER PIN HANDLING POLICY

1.1 PROHIBITED ACTIONS REGARDING CARDHOLDER PINS

All personnel are **strictly prohibited** from requesting, observing, or entering a cardholder's Personal Identification Number (PIN) at any point during a transaction or interaction.

- **1.1.1 No PIN Request:** Personnel shall never ask a cardholder for their PIN. The PIN is private and known only to the cardholder.
- **1.1.2 No PIN Observation:** Personnel shall take all reasonable steps to avoid observing a cardholder's PIN as it is entered. This includes maintaining a respectful distance and ensuring privacy shields or the physical layout of the POI device prevent visual access to the PIN pad.
- **1.1.3 No PIN Entry by Employee:** Under no circumstances shall an employee enter a cardholder's PIN into a POI device or any other system. Cardholders must always enter their own PINs.
- **1.1.4 Customer Assistance:** If a cardholder requires assistance with a transaction, personnel may guide them to the correct function on the POI device, but the PIN entry itself must be performed solely by the cardholder.

2. POINT OF INTERACTION (POI) DEVICE SECURITY INSPECTIONS, DECOMMISSIONING AND REPORTING

2.1 PERIODIC INSPECTION OF POI DEVICES

All POI devices must be periodically inspected by designated personnel to detect any signs of tampering or unauthorised substitution. These inspections shall be conducted regularly and documented.

- **2.1.1 Visual Inspection Checklist:** During each inspection, personnel must verify the following:
    - **Unexpected Attachments/Cables:** Check for any unusual or unauthorised attachments, cables, or devices plugged into the POI device that do not belong.
    - **Missing or Changed Security Labels:** Verify that all security labels are present, intact, and show no signs of alteration, removal, or damage.

- **Broken or Differently Colored Casing:** Inspect the device casing for any cracks, breaks, discolored sections, or signs that the casing has been opened or replaced.
- **Changes to Serial Number/External Markings:** Confirm that the device's serial number and any other external identifying markings match official records and show no signs of alteration.
- **Overall Appearance:** Ensure the device's overall appearance is consistent with other authorised devices and does not appear to have been swapped with a different model or type.

2.2 PROCEDURES FOR DETECTING AND REPORTING TAMPERED OR MISSING POI DEVICES

Personnel are responsible for the immediate detection and reporting of any suspected POI device tampering or missing devices.

- **2.2.1 Detection:**
  - Any observation of an unexpected attachment, missing/changed security label, broken/differently colored casing, altered serial number, or any other physical anomaly on a POI device must be considered a potential tampering incident.
  - Any POI device that is unaccounted for or cannot be located must be considered missing.
- **2.2.2 Immediate Action Upon Detection of Tampering:**
  - Immediately remove the suspected tampered device from service.
  - **Do not turn off or unplug the device** unless absolutely necessary to isolate it, as this may erase forensic data.
  - Place the device in a secure, isolated location (e.g., locked cabinet) to preserve it for forensic analysis.
  - Inform your supervisor or manager immediately.
- **2.2.3 Immediate Action Upon Detection of a Missing Device:**
  - Confirm the device is indeed missing after a thorough search.
  - Inform your supervisor or manager immediately.
- **2.2.4 Reporting Procedure:**
  - All suspected tampering incidents or missing devices must be reported to Peach Payments Support Team (support@peachpayments.com) immediately or as soon as the situation allows such that they can proceed with decommissioning of the device,

    - The report must include:
        - Date and time of detection.
        - Location of the device (or last known location if missing).
        - Device serial number or other identifying marks.
        - Detailed description of the suspected tampering (e.g., what was observed).
        - Names of personnel who detected the issue.
- **2.2.5 General Decommissioning of POI Devices**
    - For general POI decommissioning such as device EOL, general maintenance or repair, or other similar scenarios, please contact Peach Payments Support (support@peachpayments.com) to ensure correct procedures are followed for the return and decommissioning of devices.

3. PERSONNEL TRAINING ON POI DEVICE SECURITY

3.1 TRAINING FOR POI ENVIRONMENT PERSONNEL

All personnel working in environments where POI devices are used must receive regular training on how to be aware of and respond to attempted tampering or replacement of POI devices. Training shall include:

- **3.1.1 Verifying Third-Party Personnel Identity:**
    - Before granting any third-party individuals (e.g., repair technicians, maintenance personnel, vendor representatives) access to modify or troubleshoot POI devices, personnel must:
        - **Require official identification:** Request a valid company ID, work order, or letter of authorisation from their organisation.
        - **Verify with management/vendor:** Contact their supervisor or the POI device vendor directly (using independently verified contact information, not information provided by the individual) to confirm their identity and the scheduled service.

        - **Escort and Monitor:** All third-party personnel must be escorted and monitored by a designated employee while they are in proximity to or working on POI devices.
- **3.1.2 Device Installation, Replacement, and Return Verification:**
    - Procedures are in place to ensure POI devices are not installed, replaced, or returned without proper verification. This includes:
        - **Matching Serial Numbers:** Before accepting a new or replacement device, personnel must verify that the serial number on the device matches the serial number documented in the delivery manifest or service order.
        - **Visual Inspection of New Devices:** New or replacement devices must undergo a basic visual inspection upon receipt to ensure they appear legitimate and untampered (e.g., no unusual markings, intact packaging).
        - **Documenting Device Changes:** All device installations, replacements, and returns must be thoroughly documented, including serial numbers, dates, and names of involved personnel.
- **3.1.3 Awareness of Suspicious Behavior:**
    - Personnel must be vigilant and aware of suspicious behavior around POI devices, including but not limited to:
        - Individuals loitering near devices without apparent purpose.
        - Individuals attempting to obscure their actions while near devices.
        - Any person attempting to physically manipulate devices or connect unauthorised equipment.
        - Individuals attempting to distract personnel while another person interacts with a device.
        - Non-personnel attempting to access devices during non-business hours.
- **3.1.4 Reporting Suspicious Behavior and Indications of Device Tampering:**
    - Any observation of suspicious behavior or indications of potential device tampering must be **immediately reported** to a supervisor or manager.
    - Do not confront suspicious individuals directly. Prioritise personal safety and discreetly report the observation.