RIT | Rochester Institute of Technology

RIT PCI Device Inventory and Inspection Policy

1.0 Purpose

- The purpose of this policy is to define RIT Business Unit requirements for maintaining an inventory of and inspecting point-of-interaction (POI) devices that process payment card transactions.

2.0 Scope

- This policy applies to all RIT Business Units that use POI devices to capture credit and debit card data.

3.0 Policy

3.1. POI Device Inventory

- Business Units must perform an inventory of POI devices in their location, every six months
- At a minimum, Business Units must document the following for each device:
    - Device Location (e.g. Front Desk, Bill's Office)
    - Serial Number (generally located on bottom of device)
    - Model Name and Number (e.g. Ingenico IPP 350, Verifone VX520)
    - Status (e.g. Deployed, Awaiting Deployment, Inactive Device)
    - Number and Type of Connections (e.g. 1 phone line, 1 USB, etc.)
    - Security Description (e.g. device is in location that locks after hours)
- The POI Device Inventory for each Business Unit must be updated whenever a change is made (e.g. if a new device is deployed or if the location changes, etc.)
- Business Units must share their POI Device Inventory with the PCI Team upon request.

3.2 POI Device Inspection

- All POI devices must be inspected at least once a year, and this inspection must be documented.
    - Business Units with Point-to-Point encrypted (P2PE) POI Devices (e.g. Bluefin, Worldpay, FreedomPay) may require more frequent inspections.
        - Business Units with P2PE POI devices are required to understand the requirements defined in the Point-to-point Instruction Manual (PIM) distributed by the Business Unit's P2PE solution provider.
- At a minimum, documented Inspections must include the following:
    - Device Location
    - Serial Number
    - Name of Reviewer
    - Date of Review

- Business Units are encouraged to visually inspect devices before the first use of each day for any signs of tampering such as scratch marks, new cables, new/unknown devices attached to POI device or cables, etc.).
- If a Business Unit suspects tampering they must immediately report the incident to PCI Team.

4.0 Enforcement

- POI Inventories will be reviewed annually when Business Units are reviewed for PCI compliance by the RIT PCI Team.
- Failure to maintain an inventory and complete the documented inspections could result in the RIT losing the ability to accept payments via debit and credit card.

5.0 Definitions

- PCI – Payment Card Industry; PCI sets standards that must be followed by all business units who collect payments via credit cards and debit cards
- PCI Team – Controller's Office, ISO and ITS are responsible for establishing and enforcing PCI policy at RIT
- Business Unit – A department at RIT that processes credit and/or debit card transactions
- POI Device – Point-of-interaction device; where credit/debit cards are swiped/dipped and/or phones are tapped
- P2PE – point-to-point encrypted solution that provides encryption at the point of swipe/dip/tap/manual entry; P2PE provides ability to integrate with sales software while limiting PCI requirements
- PIM – point-to-point instruction manual provided by P2PE vendor outlining compliance requirements specific to POI device

6.0 Associated Files

- Inventory and Inspection – Template – editable template for individual Business Units to define their POI Device Inventory and track inspections

7.0 Revision History

- April 2019 – format with new policy template
- November 2024 - changed inventory frquency to every six month instead of a year, changes in PCI team members and made changes to tempering reporting.