Procedure Title	Point of Interaction (POI) Device Inspection
Procedure Unit Owner	Office of the Bursar Cash Operations
Related Policy	PCI DSS Point of Interaction (POI) Devices
Effective Date	11/18/2025
Date Last Updated	09/03/2025
Contact Information	cashoperations@uconn.edu
Official Website	https://bursar.uconn.edu/departments/cash-operations/

PURPOSE

To establish PCI DSS compliant procedures for managing the physical security and integrity of Point of Interaction (POI) devices that process sensitive cardholder data.

STEP BY STEP PROCEDURES

Departments must document standard operating procedures for maintaining their POI devices. Procedures should be reviewed and updated at least annually. The procedures must meet current PCI DSS requirements for restricting physical access to cardholder data including the below items:

1. **Device Inventory**
   Maintain a centralized inventory of all POI devices using the standardized POI Device Inventory Log which includes:
   - Device type, make, and model
   - Serial number or unique ID
   - Physical location
   - Assigned custodian
   - Pin Transaction Security (PITS) expiration date
   - Pictures of device to use as baseline photos

2. **Daily Physical Inspections**
   Perform visual daily inspections for:
   - Signs of tampering (e.g., broken seals, added hardware, changed wires, unusual gaps)
   - Unauthorized substitution or relocation of device
   - Comparison of devices to baseline photos

3. **Logged Inspections**
   Conduct and log more robust, formal inspections by utilizing the standardized POI Inspection Log. Determining the frequency of logged inspections should be risk-based and follow the below guidelines. The risk assessment should be reviewed annually or upon significant changes.

Frequency Used	Location of Device	Suggested Frequency
Daily	Public Area or Secured Location	Daily
Weekly	Public Area	Daily
Weekly	Secured Location	Weekly
Monthly	Public Area	Daily
Monthly	Secured Location	Monthly
Upon Sign Out	Secured Location	Upon Sign Out and Sign In

4. Staff Training

All staff using POI devices must receive training. Training should be documented and updated at least annually and include:

- Identify signs of tampering or suspicious behavior
- Identify unauthorized substitution of devices
- Verify identity of maintenance personnel before granting access to devices
- How and who to report anomalies or suspicious behavior

5. Incident Response

Any suspected tampering must trigger UConn's Incident Response Plan. Initial steps by the department should include:

- Immediately disconnect device and stop usage
- Contact PCI Team – Cash Operations, IT Security

REFERENCES

PCI DSS Requirements for Restricting Physical Access to Cardholder Data
POI Device Inventory Log
POI Device Inspection Log
UConn Incident Response Plan