BYU PCI Device Inspection Procedure

According to the Payment Card Industry Data Security Standard (PCI DSS), **Requirement 9: Restrict Physical Access to Cardholder Data**, the following requirements are to be maintained for all point-of-sale devices capable of in-person transaction processing:

Requirement 9.5.1: Point of Interaction (POI) devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

- Maintaining a list of POI devices.
- Periodically inspecting POI devices to look for tampering or unauthorized substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

Requirement 9.5.1.1: An up-to-date list of POI devices is maintained, including:

- Make and model of the device.
- Location of device.
- Device serial numbers or other methods of unique identification.

Requirement 9.5.1.2: POI devices surfaces are periodically inspected to detect tampering and unauthorized substitution.

BYU will meet Requirement 9 by keeping an inspection log to document all inspections of the POI devices. Inspections will be completed as follows:

- All personnel handling in-person transactions will be trained annually on device inspections in the BYU PCI Training module.
- The inspections are the responsibility of each applicable merchant department. The merchant contact for each department will be responsible for reporting the inspections but may delegate the inspections to designated personnel.
- Inspections, by designated personnel, will be completed monthly or more often if desired by the merchant department.
- Inspectors will record their findings in their log which includes inspection of the following:
    - Date of the inspection
    - Inspector's first and last name
    - Device Serial Number
    - Location

    - Card Reader (swipe & dip)
    - Cords
    - Ports
- Inspectors will notate any changes on the log if:
    - The device has been replaced by appropriate BYU personnel.
    - The device shows signs of tampering such as damage to the device, cords, or ports.
    - The device shows signs of tampering such as unauthorized cord adaptors or wires in the swipe and dip readers, or new face plates, or newly attached devices such as cameras.
    - The device shows signs of tampering due to an error message on the device display.
- Inspection logs will be retained for at least 18 months but may be stored indefinitely.
- Inspectors will follow the BYU Incident Response Procedure for any device that shows evidence of tampering.
    - Inspectors will ensure the operation of tampered equipment is suspended immediately.
    - Inspectors should report missing devices, or any suspicious activity regarding device maintenance or replacement that is not completed by an approved BYU employee.

Merchant Departments may choose to log their Device Inspections in a way that suits their area including, but not limited to the following:

- Spreadsheets of devices kept by the department that includes all information listed above.
- The BYU PCI Device Inspection Log.
- Bluefin P2PE Manager inspection records (for applicable departments only).
- A log of their own making that includes all information listed above.

Merchants will upload their documents to the designated Box file for their department located in the PCI Compliance Program Box file.

Related Procedures & Guidance:
BYU PCI Data Security Procedures
Information Security Major Incident Response Plan
PCI Incident Response Guidance

02/2026