BUSINESS UNIT PCI SECURITY GUIDE

04/01/2024

Table of Contents

Objective

This document defines the framework for SodexoLive! to conduct business assuring the business unit complies with the ITP-150 Payment Card Industry (PCI) Policy 4.0.

Scope

The procedural guidelines represented in this document and will assist the reader with understanding how to maintain PCI compliance and to understand what artifacts may be asked of them during an audit.

Roles

Qualified Implementation Resource – This resource from Emerging Technology will ensure the business unit is prepared to complete the activities covered in this document.

General Manager – Ensure that the business unit maintains compliance with ITG-250 Business Unit PCI Security Guide 4.0.

Employees – Complete assigned training and provide appropriate acknowledgement to their manager and ensure they conduct assigned tasks as expected.

Managers – Monitor overall compliance within their team(s) and assist the GM with maintaining evidence of compliance.

Point of Sale (POS) Guidelines

SodexoLive! units utilizing POS systems must follow these procedures and provide evidence attesting to it. This will position SodexoLive! to meet their compliance obligations with the Card Brands.

- Devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution.
- A list of devices maintained and periodically inspected to look for tampering or substitution, and employees trained to be aware of suspicious behavior and to report tampering or substitution of devices.

To assist with this the following activities must be completed as described below.

Maintaining a POS Inventory

It will be the responsibility of the assigned QIR (Qualified Implementation Resource) from Emerging Technology team at the time of installation.

The inventory must contain the following information.

1. Make, model of device and associated payment device.
2. Location of devices and condition.
3. Device serial number or other method of unique identification.
4. Application/version number
5. LAN connection type.

The inventory will be reviewed with the business unit resource responsible for the POS devices. A copy of the inventory will be provided to the business unit resource responsible for maintaining an accurate inventory taking into account when devices are added, relocated, decommissioned, etc.

Inspection of POS Devices

Please note that the appropriate steps necessary to inspect POS devices will vary based on the POS solution in place and should be documented in the vendor documentation provided by the QIR who performed the installation.

Device surfaces need to be inspected periodically to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

1. Inspect POS devices for tampering periodically in accordance with the vendor documentation.
2. Log the inspection date, who performed it and what the findings were (utilize a template for logging the inspections).
3. Maintain the inspection log and provide it to IT Auditors as requested.

Training of Employees

Personnel must be trained to be aware of attempted tampering or replacement of devices.

Note: Each POS solution vendor may have specific training to their solution. Please refer to the vendor supplied documentation for specific training for your system.

Best Practices include:

1. Conduct a training session for new employees within 30 days of hire.
2. Conduct refresh training annually or as significant changes occur to the POS solutions.
3. Maintain a training log using the template and log the date of training, names and who conducted the training and provide copies to IT Auditors when requested.

Security Awareness Training

This section describes the approach the business units are required to implement for Security Awareness Training.

ITG-251 PCI Security Awareness Training 4.0 is designed to satisfy the need for the business unit training. It's recommended that the BU follow the steps below to complete the training.

Here are the steps to complete this training.

1. Email a copy of the document to employees annually and maintain a copy of the email and distribution list.
2. Email a copy of the document to new hires within 30 days of hire and maintain a copy of the email and distribution list.
3. Post a copy of the ITG-251A PCI Security Awareness 4.0 on a centrally located bulletin board preferably in a break room and/or near the time clock.

Controls Observed

PCI Requirement 9.5.1	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.
PCI 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 number or other methods of unique identification.
PCI Requirement 9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.
PCI Requirement 9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.
PCI Requirement 12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.

Revision History

Date	Description	Approver
6/15/2022	Formalized the guidelines.	Michael Porter
5/18/2023	Completed an annual review and updated the Security Awareness section.	Wayne Duprey Michael Porter
10/18/2023	Revised to change Centerplate to SodexoLive!	Brad Kellett
03/12/2024	Reviewed/Modified to account for PCI SSC 4.0 changes effective 4/1/2024.	Brad Kellett