Introduction to PCI (at a Glance)

Overview

All Sodexo Live locations that accept credit/debit card payments are considered merchant locations and must process those payments in a secure manner. It is the responsibility of each location to maintain compliance with the Sodexo Live policies and the Payment Card Industry Data Security Standard (PCI DSS) established by the Payment Card Industry Security Standards Council (PCI SSC).

Sodexo Live's PCI DSS Compliance Program addresses requirements of the PCI SSC, including:

- Security Awareness Education (required PCI DSS Security Training and Attestation)
- System Vulnerability Scans
- System Penetration Testing
- Periodic Reviews and Audits
- Annual PCI SAQ (Self-Assessment Questionnaire)

1. PCI DSS Security Training and Attestation

Per PCI DSS requirement 12.6, Sodexo Live requires all location personnel interacting with the Cardholder Data Environment (CDE) in any manner (from the initial entry to the final reconciliation) to complete an annual training and attestation. This mandatory requirement includes student employees, contractors, and volunteers.

Individuals who have not completed training and attestation are not permitted to process Cardholder Data (CHD) on behalf of Sodexo Live interests. Locations using untrained or unattested individuals to process CHD may have their merchant account revoked.

2. Periodic Reviews and Audits

Sodexo Live corporate Audit may perform periodic reviews or audits of location operations to ensure that locations comply with PCI DSS and the Sodexo Live's risk is reduced. Failure to cooperate with such activities may result in merchant account usage being revoked.

Locations should also routinely review their procedures and equipment, including physically inspecting card processing equipment to ensure devices have not been substituted or tampered. This Merchant Location Device Inspection Checklist can be used for your inspections.

3. Annual PCI SAQ (Self-Assessment Questionnaire)

All Sodexo Live locations are required to validate PCI-DSS compliance at least annually by completing the appropriate SAQ in a timely manner. A questionnaire must be completed for each Merchant account, and a new questionnaire must be filled out whenever any of the following have occurred:

- payment processing system changes
- a year has elapsed since your last SAQ
- upon Operations request