	TOPIC TITLE: Payment Card Industry (PCI) POLICY	
	POLICY NUMBER: ITP-150	**POLICY OWNER:** VP Emerging Technology
	SECTION: ITP-100 General Policies	**VERSION DATE:** 04/1/2024
DATE: The date when this policy is posted to the Internal IT (Information Technology) Policies repository:		

Purpose

This policy provides guidance for maintaining compliance with the PCI (Payment Card Industry) SSC (Data Security Standard) Standard. This policy will reduce the risk associated with the processing, transmitting, or storing of card holder data and to satisfy the requirement(s) put forth by the Card Brands (AMEX, Visa, Master Card, and Discovery).

Scope

SodexoLive! employees of the company, including consultants and third parties employed or retained by SodexoLive! that process, transmit or stores card holder data will be required to adhere to this policy and their business unit will be assessed annually against the PCI SSC Standards in place at the time of assessment. In addition, the Information Technology resources including Emerging Technology, IT POS (Point of Sale) Operations and IT Audit resources must comply with this policy.

Please note that business units whose client owns and operates the entire network and POS solution will need to demonstrate PCI compliance (provide a current Attestation of Compliance annually) if they are on a SodexoLive! MID (Merchant ID).

Policy

General

The SodexoLive! standard is to deloy P2PE Products (P2PE Solutions, P2PE Components, and P2PE Applications) to business units that process, store or transmit credit card data. Business responsibilities include managing vendor upgrades to the PCI SSC approved POS solution(s), securely maintain approved payment devices and will be subject to an annual PCI assessment to determine overall compliance with the current PCI SSC requirements and this policy.

Emerging Technology

1. Participate in the PCI QIR (Qualified Integrator and Reseller) program managed by PCI Security Standards Council, LLC (“PCI SSC”),and maintain the guiding principles procedures for the secure installation and maintenance of all payment applications in a manner that supports dompliance.
2. Maintain accredited QIR status serve as an important role in the payments and information technology value chain. QIRs help their merchant customers improve payment data security and reduce risk by implementing the critical security controls to mitigate the most common causes of payment data breaches.
3. Complete an accurate Report of Services following a POS installation/upgrade/annual health check and submit this artifact to Emerging Technology management.
4. Complete an accurate QIR Implementation Statement and submit this artifact to Emerging Technology management.
5. Submission of artifacts are required within 10 days of a new implementation/upgrade/health check..
6. Support the IT Auditor performing an annual PCI assessment as needed.

Business Units

1. Complete an annual review of the Security Policy and submit an attestation confirming compliance with this requirement.
2. Complete an annual Security Awareness Training program and submit an attestation confirming compliance with this requirement.
3. Maintain an accurate POS device inventory (provided by Emerging Technology Manager during installation).
4. Inspect POS devices periodically for tampering and maintain a log demonstrating compliance with this requirement.
5. Train resources to recognize device tampering as needed based on hiring practices and changing technology. And maintain a log of who was trained demonstrating compliance with this requirement.
6. Support the IT Auditor performing an annual PCI assessment as needed.
7. Submit artifacts when requested to demonstrate compliance.

Corporate Support Center

1. Complete an annual review of the Security Policy and submit an attestation confirming compliance with this requirement.
2. Complete an annual Security Awareness Training program and submit an attestation confirming compliance with this requirement.
3. Develop an accurate Network Diagram for each of the business units.
4. Conduct quarterly PCI scans using an ASV (Approved Scanning Vendor) and remediate findings as needed.
5. Remediate vulnerabilities identified for POS business units as required.
6. Support the IT Auditor performing an annual PCI assessment as needed.
7. Submit artifacts when requested to demonstrate compliance.

Information Technology

1. Complete an annual review of the Security Policy and submit attestation confirming compliance with this requirement.
2. Complete an annual Security Awareness Training program and submit attestation confirming compliance with this requirement.
3. Remediate identified vulnerabilities as required.
4. Support the IT Auditor performing an annual PCI assessment as needed.
5. Submit artifacts when requested to demonstrate compliance.

Information Technology Audit

1. Complete an annual review of the Security Policy and submit an attestation confirming compliance with this requirement.
2. Complete an annual Security Awareness Training program and submit an attestation confirming compliance with this requirement.
3. Complete the annual (or when a significant change occurs) PCI self-assessment questionnaire and attestation of compliance.
4. Coordinate activities with the AMEX card brand as required.

Supporting Documentation

1. ITG 250 Business Unit PCI Security Guide 4.0
2. ITG 251 PCI Security Awareness Training 4.0
3. ITG 251A PCI Security Awareness Poster 4.0

Enforcement

Employees who fail to comply with this policy may be subject to constructive counseling up to and including termination of employment.

Review and Update

This policy will be reviewed and/or updated at least annually or when there are significant changes impacting the content of this policy.

Responsibilities

Employee: Employees are required to be familiar with and comply with Company policies. The Company expects employees to report any violations of this policy to one's supervisor or as otherwise provided in the policy.

Management: Managers are required to be familiar with and enforce this policy, and to take appropriate action when violations of policy occur or are reported. Managers are also responsible for ensuring there are no retaliatory actions because of an employee reporting any policy violation.

Human Resources: Human Resources representatives are responsible for being familiar with this policy to provide appropriate guidance and to take appropriate action when violations of policy are reported.

Interpretation: Chief Financial Officer retains the right to interpret, revise, and/or amend this policy at any time, subject to ITP-101 Policy on Policies.

Revision History

Date	Description	Reviewer
6/15/2022	Formalized the guidelines.	Michael Porter
1/09/2023	Peer review, some grammar corrected.	Terry Fitzgerald
1/26/2023	Added policy clarification addressing client owned network and POS system and utilizing SodexoLive! MID (Merchant ID). Made final changes to policy sections and Supporting Procedures.	Brad Kellett
5/22/2023	Completed an annual review and updated as needed.	Wayne Duprey Michael Porter
10/18/2023	Revised to change Centerplate to SodexoLive!	Brad Kellett
3/12/2024	Reviewed/Modified for PCI SSC 4.0 (effective 4/1/2024). Version date modified to 04/01/2024.	Brad Kellett