SNOWBE ONLINE Policy#SP-1

PCI DSS Policy

Michael Kohronas:

<PCI DSS>

Version #3

DATE: 06/2024

<PCI DSS> – V 3.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Michael Kohronas
DATE – 06/2024

Table of Contents

Policy

PCI-DSS (Payment Card Industry Data Security Standard) is a privately managed set of data security regulations for the credit card processing sector. PCI-DSS aims to safeguard cardholder data during and after transactions. And the regulations set down a strict set of compliance criteria to achieve this goal.

Scope

This policy applies to all staff, contractors, and interns who process, store, or transmit cardholder data for SnowBe. This policy encompasses all systems handling and protecting card information.

Definitions

Cardholder Data – Any personal information that is associated with a cardholder. This information can include credit card number, name, expiration date, CVS number, and Primary Account Number

Encryption – The process of securing data by transferring it to a unreadable language that can only be unscrambled with a decryption key.

PCI DSS – A set of security standards designed to protect card information by ensuring all organizations accept, process, store, or transmit credit card information in a safe and secure manner.

PCI Compliant Devices – Any devices that is used to collect or store cardholder information which follows PCI compliance.

Roles & Responsibilities

All Employees, contractors, or interns – Follow PCI compliance when handling cardholder information and ensure there are no unknown third-party devices on card readers that can hinder security.

CISO – Oversee the development, implementation, and maintenance of the PCI Compliance Policy.

IT Security team – Ensure that all cardholder data is being collected and stored properly and reporting and resolving any data or devices that aren’t meeting PCI compliance.

Policy

The purpose of the PCI DSS policy is to ensure that SnowBe can effectively protect cardholder data, use compliant card readers, and properly store transaction history.

Access management – Access controls determine who has access to the CDE, when they have access and the actions they can take. This applies to anyone who can access cardholder data. It also includes rules for device usage, both on-site and remotely. Document any authorization systems in use, including attribute or role-based access controls.

Account management – Details how user accounts are created, managed, and deleted. This includes a mandatory agreement to comply with security policies. Accounts should have unique IDs. Account sharing should be prohibited. This section may include details about multi-factor authentication (MFA) or 2FA systems. It may also deal with third-party or vendor accounts if applicable.

Data encryption – Defines the encryption standards used to protect customer data, as well as how to store encryption keys and sensitive authentication data.

Data protection and retention – Includes guidelines for the retention and secure deletion of cardholder data. This should include controls to protect payment card data such as Primary Account Numbers (PANs), as well as encryption of all other credit card data.

Firewalls – How firewalls are configured, and how firewall protection guards secure zones within the CDE. Includes firewall requirements for remote devices. May also feature details about segmentation to create DMZs for the most sensitive data.

Device management – Details how the organization manages digital and physical assets to guard data. Includes devices to take payments and communicate cardholder data. Also includes the need to inventory all devices and log device maintenance activity. Backup security is also part of this section.

Network management – Deals with network infrastructure within the scope of the CDE. Standard security configurations should enforce device patching and changing vendor defaults. Companies should create data flow diagrams to track cardholder data throughout the network. Every device should be covered by anti-virus software. Encryption should protect wireless networks, with specific controls for wireless access points.

Activity logging – Demonstrates that the organization keeps audit trails for all devices and users. Mandates the use of timestamps for all access requests and actions. Audit trails should be secured from tampering. And logs must be reviewed to detect security issues.

Incident response – How the organization responds during security incidents. Under PCI-DSS rules, the organization requires a response plan that is tested annually. Security teams should be available to respond to security alerts at all times.

Physical access – Any devices within the scope of the CDE require access controls. Companies should also closely monitor physical access via cameras and sensors. Physical access should be determined by role, with time-limited access to devices hosting cardholder data. Visitor management should identify and authorize all external visitors.

Remote access – There should be separate controls for remote access to the CDE. This includes MFA and the use of data tracking to prevent the movement of sensitive data. The organization should approve all remote devices. It should include rules about storing sensitive authentication data and avoiding insecure public networks.

Software development – Includes rules about the creation and maintenance of CDEs. This section mainly deals with the responsibilities of developers. All personal cardholder data should be removed during testing processes. App developers should follow secure coding practices. And there must be specific controls to protect public-facing web applications.

Vulnerability management – This section defines procedures to detect security vulnerabilities. It can be included as a sub-section under security controls or added as a separate section. In either case, this section should cover PCI-DSS requirements such as:

Network scanning – Network scans should be carried out quarterly. Organizations should enlist Approved Scanning Vendors (ASVs) to execute network scans. The scan should assess vulnerabilities according to severity. Re-scanning may be needed until all vulnerabilities have been fixed.

Regular patch management – IT teams should update all software within the CDE as soon as new security patches are available. Network scans should establish the need for software updates if patches are not already in place.

Penetration testing –The policy may require annual penetration testing by an ASV. This simulates common network attacks and suggests areas of improvement. Intrusion detection/prevention systems (IDPS) should detect incoming threats and apply controls to neutralize attacks.

Training –Explains training and employee awareness programs in place to meet every PCI-DSS requirement. Training should revolve around data security responsibilities, and programs should cover all users with CDE components.

Monitoring – The policy should define processes to monitor PCI compliance. This includes regular audits in line with the organization's PCI level. It also includes threat assessments and incident reporting.

Exceptions/Exemptions

PCI-DSS (Payment Card Industry Data Security Standard) is a privately managed set of data security regulations for the credit card processing sector. PCI-DSS aims to safeguard cardholder data during and after transactions. And the regulations set down a strict set of compliance criteria to achieve this goal.

Exceptions to this Policy will be considered on a case-by-case basis and do not guarantee approval. To request an exception, please submit a written request to the IT Director outlining the following:

How to Request Exceptions/Exemptions?
To request an Exception or Exemption from a Policy that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The IT Director, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions. Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement

The failure to comply with policies, Policys, or Policys will result in a warning or disciplinary action depending on the severity of the infraction.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
v1	06/06/2024	Michael Kohronas		Added the exception and exemption and enforcement as a group
V2	06/07/2024	Michael Kohronas		Fixed issues with text size and font, added name and date to header,
V3	06/24/2024	Michael Kohronas		Created PCI DSS policy

Citations

https://nordlayer.com/learn/pci-dss/pci-compliance-policy/