SNOWBE ONLINE #007

PCI DSS POLICY

Your name: Group 2

PCI DSS Policy - Version # 1

DATE: 10-5-25

Table of Contents

Purpose

This document provides guidance on protecting payment and card data as well as consumer information. Failure to protect this information can result in financial loss for customers, suspension from credit card processing privileges, fines, damage to the company's reputation.

Scope

This policy applies to those involved with payment card handling such as all employees, systems, third-party agents, service providers, and affiliates that store, transmit, and have access to SnowBe customer financial data. As well as any hardware devices like servers, end point devices, software, and network devices that handle SnowBe data.

Definitions

Cardholder

Individual who owns and benefits from the use of a membership card, particularly a payment card.

Cardholder Data (CHD)

Elements of payment card information that must be protected, including primary account number (PAN), cardholder name, expiration date, and the service code.

Cardholder Name

The name of the individual to whom the card is issued.

Expiration Date

The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

Service Code

Permits where the card is used and for what.

Disposal

CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, and USB storage devices in accordance with the *Record Retention and Disposition Policy*. The approved PCI DSS disposal methods include cross-cut shredding, incineration, and approved shredding and disposal service.

Merchant

A department or unit (including a group of departments or a subset of a department) approved to accept payment cards and assigned a merchant identification number.

Payment Card Industry Data Security Standards (PCI DSS)

The security requirements defined by the Payment Card Industry Data Security Standards Council and the major credit card brands including Visa, MasterCard, Discover, American Express, and JCB.

PCI Compliance Committee

Group composed of representatives from Financial Management, Information Security Office, Office of the Vice President and Chief Information Officer, Internal Audit, and SnowBe's merchants.

Primary Account Number (PAN)

Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account and includes a check digit as an authentication device.

Self-Assessment Questionnaire (SAQ)

Validation tools to assist merchants and service providers report the results of their PCI DSS self-assessment.

Sensitive Authentication Data

Additional elements of payment card information required to be protected but never stored. These include magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN or PIN block.

CAV2, CVC2, CID, or CVV2 data

The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

Magnetic Stripe (i.e., track) data

Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

PIN or PIN block

Personal identification number entered by the cardholder during a card-present transaction, or encrypted PIN block present within the transaction message.

Roles & Responsibilities

Members of the SnowBe's Company

- Safeguard cardholder data.
- Report occurrences of possible incidents and data breaches to your supervisor or the SnowBe information Security Officer.
- Review and comply with the following SnowBe policies:
  - *SnowBe IT Password*
  - *Protection of SnowBe Data*

PCI Compliance Committee

- Monitor SnowBe's compliance with PCI DSS requirements.
- Act as a steering committee for PCI DSS.
- Support PCI DSS compliance efforts.
- Review the required annual SAQ self-assessment.

SnowBe Information Technology (SBIT)

- Maintain security standards required by PCI DSS.
- Keep current with PCI DSS regulations and make changes to systems and processes, as appropriate.
- Consult on technical PCI DSS issues.
- Assist with mandatory annual training sessions.

Policy, Compliance and Internal Controls

- Maintain an inventory of all SnowBe locations and departments that process payment card transactions using an approved merchant account, SnowBe Marketplace, or other compliant methods.
- Provide and monitor annual training that meets the PCI DSS requirements.

- Coordinate completion of the annual self-assessment documents (SAQs).
- Collect departmental PCI procedures as part of the annual SAQs.
- Evaluate compliance with PCI as part of scheduled cash handling reviews; this is a shared responsibility with Financial Management.

Financial Management

- Keep current with PCI DSS regulations and make changes to processes, as appropriate.
- Maintain the inventory of all State devices (i.e., analog, cellular, Bluefin), merchant ids, and terminal ids along with activation status.
- Evaluate compliance with PCI as part of scheduled cash handling reviews; this is a shared responsibility with Policy, Compliance and Internal Control.

Department and Unit Heads (who accept payment card payments other than through approved online methods)

- Review and comply with the following SnowBe policies:
  - *Credit/Debit Card Merchant Requirements*
  - *Safeguarding Cash and Cash Equivalents*
- Complete the required annual PCI self-assessment (SAQ).
- Complete the annual PCI training through Financial Management.
- Require appropriate staff to complete the annual PCI training through Financial Management.
- Maintain departmental Standard Operating Procedures (SPO) for PCI compliance and verify staff has an understanding of the procedures and their responsibilities.

Payment Card Handlers and Processors

- Follow the established cash receipts procedures for the appropriate funding source.
- Follow the Payment Card Processing Options and use PCI Compliant Devices for all card transactions.
- Complete the *Payment Card Authorization Form* when appropriate.
- Complete the annual PCI training through Financial Management.
- Review and comply with the following SnowBe policies:
  - *Credit/Debit Card Merchant Requirements*
  - *Safeguarding Cash and Cash Equivalents*

Third Party Payment Card Processors

- Provide confirmation of compliance.

Policy

This Policy has been put in place to align SnowBe with the Payment Card Industry Data Security Standards (PCI DSS) and protect the confidentiality, integrity, and availability of customer information.

Goals and PCI DSS Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti- virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

SnowBe is required to comply with all relevant standards. However, not all of the PCI DSS requirements are relevant to SnowBe. Certain SnowBe policies reduce the compliance scope, including prohibiting electronic storage of payment card information, restricting transmission through fax and email, and utilizing third-party vendors for web-based payment card processing rather than SnowBe net

Exceptions/Exemptions

Requests for an exception must be submitted in writing to consult with the IT Director or IT Manager.

The request must be detailed with information, including:

- Length of time
- Policy or standard
- Reason

And the Exception Request form must be signed by:

- CIO
- Information Security Officer
- CEO
- Commissioner

Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.

If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.

The CISO, the information security officer representing, and the commissioner must maintain constant communication during the exception. If approved, the CISO's office will send the letter of approval to the requester with details. IN the event of denial, a letter of explanation will be sent to the requestor with the reason the CISO denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

Enforcement

Failure to comply with SnowBe policies can result in disciplinary action varying from warnings to termination and legal action depending on the severity of the event. All violations will be reviewed by the IT Manager or IT Director along with the HR Department.

Enforcement levels include:

1. **Verbal Warning** - For minor or first-time violations where the issue can be corrected immediately.
2. **Written Warning** - For repeated or mild violations that can pose a potential risk to company operations or critical company data.
3. **Access Suspension** - For more serious violations that threaten the confidentiality, integrity, or availability of SnowBe systems and their data.
4. **Termination of Employment or Contract** – For intentional, malicious, or repeated violations that compromise SnowBe's systems, data, devices, or network.
5. **Legal Action** - For extreme cases such as data theft, data breach, fraud, or other criminal behavior conducted on or with SnowBe systems and devices.
    a. Levels of Non-Compliance:
        1. 1-3 months – Fines ranging from $5,000 - $10,000 a month
        2. 4-6 months – Fines ranging from $25,000 - $50,000 a month
        3. 7 months and upwards – Fines of $50,000 - $100,000 a month

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-5-25	IT Director	IT Director	Initial draft of the PCI DSS policy

Citations

University at Buffalo - https://www.buffalo.edu/administrative-services/policy-compliance-and-internal-controls/policy/ub-policy-lib/pci-compliance.html

PCI DSS Reference - https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Sprinto - https://sprinto.com/blog/pci-dss-fines/