SNOWBE ONLINE Policy# AC-1
Payment Card Industry (PCI)

Humberto Gonzalez

Version # 1.0

DATE: July 5, 2024

Table of Contents

Purpose

The purpose of this policy is to ensure that all payment card information processed, stored, or transmitted by SnowBe Online is handled securely and in compliance with the Payment Card Industry Data Security Standard (PCI DSS). SnowBe Online is committed to maintaining the highest level of security for all payment card information processed by the organization. This policy outlines the responsibilities and requirements for protecting cardholder data and ensuring compliance with Payment Card Industry Data Security Standards (PCI DSS).

The PCI DSS is a mandated set of requirements agreed upon by the major credit card companies. The security requirements apply to all transactions surrounding the payment card industry and the merchants or organizations that accept these cards as a form of payment.

SnowBe Online must comply with the PCI DSS in order to accept card payments and avoid penalties. This policy and additional supporting policies:

- Provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions
- Reduce the institutional risk associated with the administration of payment cards
- Promote proper internal control
- Promote compliance with the PCI DSS

Scope

This policy applies to all employees, contractors, and third-party entities affiliated with SnowBe Online. It covers all digital and physical assets, including the online sales platform hosted on AWS, company databases containing customer information and purchase history, multiple storefronts in the United States and Europe, desktop and laptop computers used in the Los Angeles main office, and on-premise and AWS servers that manage various business functions.

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  The date on which a card expires and is no longer valid.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 UB 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

All Members of the SnowBe Online Community:

- Safeguard cardholder data.
- Report occurrences of possible incidents and data breaches to your supervisor or the SnowBe Online
- Information Security Officer.
- Review and comply with relevant security policies.

PCI Compliance Committee:

- Monitor SnowBe Online’s compliance with PCI DSS requirements.
- Act as a steering committee for PCI DSS.
- Support PCI DSS compliance efforts.

- Review the required annual Self-Assessment Questionnaire (SAQ).

SnowBe Online Information Technology (IT):

- 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 Online departments that process payment card transactions using an approved merchant account or other compliant methods.
- Provide and monitor annual training that meets the PCI DSS requirements.
- Coordinate completion of the annual SAQ documents.
- Collect departmental PCI procedures as part of the annual SAQs.
- Evaluate compliance with PCI as part of scheduled cash handling reviews in collaboration with Financial Management.

Financial Management:

- Keep current with PCI DSS regulations and make changes to processes as appropriate.
- Maintain the inventory of all devices, merchant IDs, and terminal IDs along with activation status.
- Evaluate compliance with PCI as part of scheduled cash handling reviews in collaboration 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 relevant policies.
- Complete the required annual PCI 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 (SOP) 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.
- Use PCI Compliant Devices for all card transactions.
- Complete the annual PCI training through Financial Management.
- Review and comply with relevant policies.

Third-Party Payment Card Processors:

- Provide confirmation of compliance.

Policy

SnowBe Online is committed to complying with the PCI DSS to protect cardholder data and maintain secure processing environments. The following measures are implemented to achieve compliance:

1. **Build and Maintain a Secure Network:** Install and maintain a firewall configuration to protect cardholder data. Do not use vendor-supplied defaults for system passwords and other security parameters.
2. **Protect Cardholder Data:** Protect stored cardholder data and encrypt transmission of cardholder data across open, public networks.
3. **Maintain a Vulnerability Management Program:** Use and regularly update anti-virus software or programs and develop and maintain secure systems and applications.
4. **Implement Strong Access Control Measures:** Restrict access to cardholder data by business need to know, assign a unique ID to each person with computer access, and restrict physical access to cardholder data.
5. **Regularly Monitor and Test Networks:** Track and monitor all access to network resources and cardholder data. Regularly test security systems and processes.
6. Maintain an Information Security Policy: Maintain a policy that addresses information security for employees and contractors.
7. **Maintain an Information Security Policy:** Maintain a policy that addresses information security for employees and contractors.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	July 5, 2024	Humberto Gonzalez	Group# 4	Initial Version

Citations

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

PCI Policy- Payment Card Industry (PCI) Compliance Policy - Administrative Services Gateway - University at Buffalo

Enforcement- Sample Detailed Security Policy (bowiestate.edu)