SNOWBE ONLINE Policy 11.40

PAYMENT CARD INDUSTRY COMPLIANCE POLICY

Alex Fhermaye

PCI Compliance - 11.40

DATE: June 10, 2024

PCI Compliance Policy – V 1.2
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Alex Fhermaye
June 10, 2024

Table of Contents

Purpose

This policy document provides information to ensure that SnowBe Online complies with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the PCI DSS is to protect cardholder data. This document represents SnowBe's procedures to prevent loss or disclosure of customer information including credit card numbers. Any failures to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of the University. The PCI Compliance Team's purpose is to educate all entities in the organization's payment environment and to enforce the PCI DSS policies contained herein.

Scope

This policy applies to all campus users, external merchants, systems and networks involved with the transmission, storage, or processing of payment card data which utilize the university IT infrastructure to perform payment card processing. Payment card data includes primary account numbers, cardholder name, expiration date, service code, and sensitive authentication data.

While the law does not mandate PCI-DSS compliance, non-adherence to PCI-DSS can subject the organization to significant financial and reputational risks. Failure to comply can result in:

a) fines and penalties imposed by payment card institutions and banks.

b) monetary costs associated with legal proceedings, settlements, and judgements.

c) suspension of the merchant account and the inability to accept payment cards for payment.

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The date on which a card expires and is no longer valid.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

Chief Information Officer (CIO)

- Develop and implement the overall IT security strategy in alignment with business objectives.
- Oversee the IT department to ensure effective execution of security policies and controls.
- Ensure compliance with industry standards and regulatory requirements, including NIST 800-53 and PCI DSS.

Compliance Officer

- Ensure the company adheres to all relevant legal, regulatory, and industry standards.
- Conduct regular audits and assessments to identify compliance gaps.
- Work with other departments to implement corrective actions and maintain compliance.

IT Consultant

- Provide expert advice and guidance on IT security best practices and frameworks.
- Conduct risk assessments and develop action plans to address identified vulnerabilities.
- Assist in the implementation of security controls, policies, and procedures.

IT Security Manager

- Oversee the day-to-day operations of IT security within the company.
- Manage the IT security team and ensure the implementation of security controls and measures.
- Monitor security incidents and respond to breaches or threats.

Sales Team

- Adhere to IT security policies and procedures, particularly when accessing company systems remotely.
- Report any suspicious activities or potential security incidents to the IT security team.
- Ensure the secure handling of customer data and payment information during transactions.

System Administrator

- Manage and maintain servers, ensuring they are secure and up-to-date.
- Implement and enforce access controls to limit data access based on roles and responsibilities.
- Regularly update and patch operating systems and software to mitigate vulnerabilities.

Web Developer

- Ensure the company’s website and applications are secure and up-to-date.
- Implement security measures for online transactions and data storage.
- Regularly update and patch the WordPress shopping cart and other web components.

Policy

Storage of Sensitive Authentication Data and Cardholder Data

Storage of electronic and/or physical Cardholder Data or Sensitive Authentication Data poses significant risks and increases the number of requirements that must be satisfied to be PCI-DSS compliant.

PCI-DSS prohibits the storage of Sensitive Authentication Data, even if the data is encrypted. Sensitive Authentication Data includes the full contents of any data on a card’s magnetic stripe, card verification codes or values (CVC/CVV) and personal identification numbers (PIN).

Electronic and physical Cardholder Data shall not be stored unless there is a justified business need to do so.

Access to Cardholder Data

Cardholder Data is classified as confidential data under the CUNY Data Classification Standard. Access to Cardholder Data shall be restricted to those individuals whose job responsibilities require such access, on a strict need to know basis, as per CUNY IT Security Procedures, Section II, Access Issues. This includes fulltime, part-time, temporary, or Related Entity employees. Offices and departments that handle Cardholder Data shall define and document the roles and responsibilities of those individuals whose job functions require them to access Cardholder Data. It is crucial that individuals with Cardholder Data-handling job functions are instructed to not disclose any Cardholder Data, unless deemed necessary by a supervisor in accordance with PCI-DSS requirements and CUNY policies.

Protecting Stored Cardholder Data

SnowBe Offices and Related Entities with a justified business need to store Cardholder Data must ensure that Cardholder Data is appropriately protected. If there is a justified business need, the cardholder’s name, PAN, expiration date, and service code may be stored if protected in accordance with PCI-DSS requirements. Masking the PAN anywhere it is displayed, such as on receipts, so that only the first six and/or the last four digits are displayed is one method of protecting stored Cardholder Data. Other methods include encryption or truncation.

Retention of Cardholder Data

Any Cardholder Data that must be retained after transaction authorization based on a documented and justified business need must be kept secured and only accessible by those whose job requires that they have access to the data. For physical media containing Cardholder Data, for example, the media should be stored in a filing cabinet or safe that is always locked (during and after business hours).

Card Verification Codes or Values (CVC/CVV) and Personal Identification Numbers (PINs) must never be retained.

Cardholder Data shall not be retained for more than one year. SnowBe and Related Entities shall determine a quarterly process for identifying and securely deleting stored Cardholder Data at the end of its retention period.

Disposal of Cardholder Data

Except for Cardholder Data being retained based on a justified business need, any Cardholder Data captured to process a transaction shall be purged, deleted, or destroyed, in an irretrievable manner, immediately after authorization. The following are approved techniques for disposing of Cardholder Data:

- Paper shall be shredded, using a crosscut shredder, pulped, or incinerated.

- Digital storage media, such as CDs, DVDs, Disks, USB Drives, etc. must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure, as per PCI-DSS requirements and the CUNY IT Security Procedures.

Cardholder Data awaiting disposal must be stored in a secure container with a lock to prevent access. The container must be labeled "classified" or have a similar label to indicate the sensitivity of the data.

Receipt of Cardholder Data via End-User Messaging Technologies

SnowBe and Related Entities shall not accept Cardholder Data via end-user messaging technologies (i.e., email, instant message, text message, etc.), which are not a secure means of transmission. All forms and other documents that collect Cardholder Data shall exclude email and/or cell phone number fields as a method of submission. Cardholder Data may be accepted by fax if the machine does not store the data in memory, converts the fax into email, or is not connected to the local network (i.e., a dedicated fax machine).

If an office or department receives Cardholder Data via end-user messaging, the message shall be deleted. The office or department should compose a new email or text message to the sender advising them to refrain from sending Cardholder Data through this means of communication and provide proper credit card submission instructions. Cardholder Data received through end-user messaging shall not be processed.

Self-Assessment Questionnaire (SAQ)

Each SnowBe and Related Entity department or office that processes payment card transactions shall complete an SAQ annually to demonstrate its compliance with PCI-DSS.

Internal and External Vulnerability Scans

The entire organization and Related Entity that stores, processes, or transmits Cardholder Data through a CUNY network must conduct internal and external vulnerability scans, at least on a quarterly basis and after any significant changes, as required by the PCI-DSS. A PCI-validated Approved Scanning Vendor must conduct external vulnerability scans.

Third-Party Vendor and Service Provider Compliance

Third-party vendors and/or service providers that store, process, or transmit Cardholder Data on behalf of SnowBe or Related Entity can impact the security of the organization and must be PCI-DSS compliant. SnowBe and Related Entities shall establish a process for engaging third-party vendors and/or service providers, including confirming the third party’s PCI compliance status by checking the appropriate database (i.e., the VISA Global Registry).

All organizational and Related Entities utilizing a third-party vendor and/or service provider shall maintain an up-to-date list of all vendors and/or service providers, including a description of the services provided and the type of data shared with the third party.

Access to System Components containing Cardholder Data

SnowBe and Related Entities utilizing a system component handling Cardholder Data (i.e. Virtual Terminal or payment processing platform) shall assign a unique ID or username to each person with access and add and remove a person’s access as needed. Access for users who separate from the organization or whose job responsibilities no longer require such access shall be immediately revoked and removed. SnowBe and Related Entities shall ensure that all users secure their accounts with strong passwords, that are changed at least every 90 days. As per PCI-DSS requirements, passwords must, at least, meet the following parameters:

- A minimum password length of at least seven characters

- Contain both numeric and alphabetic characters.

SnowBe and Related Entities shall not use generic or shared user IDs and passwords and shall remove all generic user IDs prior to the utilization of the system component.

Point-of-Sale (POS) Devices and Protection against Skimming and Tampering

Point-of-Sale (POS) devices that are purchased or owned by a SnowBe or Related Entity are in-scope for PCI compliance. PCI-DSS requirements call for the protection from tampering and skimming of devices that capture payment card data via direct physical interaction. Departments or offices utilizing a Point-of Sale (POS) device that is purchased or owned shall maintain an up-to-date device inventory log, which includes the device name, model, serial #, and location of device, and shall periodically inspect the device for signs of skimming and tampering, as required by the PCI-DSS.

Disposition of Point-of-Sale (POS) Devices

SnowBe and Related Entities with Point-of-Sale devices or terminals that have been inactive for over two years shall dispose of the devices (see CUNY POS Device Inspection Guidelines and Checklist).

Protection of Networks and Systems

SnowBe and Related Entities shall establish and implement methods for protecting networks and systems that process, store, or transmit Cardholder Data, including but not limited to testing all network connections and changes to firewall configurations, maintaining network diagrams, using strong cryptography, maintaining up-to-date and actively running anti-virus programs and updating security patches in a timely manner, as required by PCI-DSS. Efforts should be made to limit and reduce the scope of required compliance with PCI-DSS by isolating and segmenting areas of the network and systems used to process Cardholder Data.

Exceptions/Exemptions

At SnowBe Online, we recognize that there may be exceptional circumstances requiring deviations from our established IT security policies. However, such exceptions/exemptions are not guaranteed approval and must be carefully evaluated to ensure they do not compromise our security posture. The following outlines the process for requesting and managing exceptions/exemptions:

How to Request an Exception/Exemption

1. All requests for exceptions or exemptions must be submitted in writing via the official IT Security Exception Request Form, available on the company net.

2. A detailed explanation of why the exception or exemption is being requested, including the specific policy or control from which the deviation is sought. The proposed duration for which the exception or exemption is needed.

Approval Process

1. The IT Security Manager will review the request to ensure it includes all required information and assess the potential risks and impacts.

2. The Chief Information Officer (CIO) has the final authority to approve or deny exceptions and exemptions. In cases involving significant risk, the CIO may consult with the Chief Executive Officer (CEO) or the IT Security Advisory Committee.

3. The applicant will be notified in writing of the decision, including any conditions or additional controls required as part of the approval.

Duration and Review

1. Approved exceptions or exemptions will typically be granted for a specified duration, not exceeding one year unless otherwise stated.

2. All active exceptions or exemptions will be reviewed periodically by the IT Security Manager to ensure that they remain necessary and that any associated risks are being adequately managed.

Enforcement

Compliance with the IT security policy and any granted exceptions or exemptions will be monitored continuously. Any deviations from approved exceptions or exemptions must be reported immediately to the IT Security Manager.

Failure to follow the IT security policy, including the proper procedure for requesting and adhering to exceptions or exemptions, may result in disciplinary actions. Penalties may include, but are not limited to, revocation of access privileges, formal reprimand, or other disciplinary actions up to and including termination of employment.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	June 4, 2024	Alex Fhermaye		Initial Submission for review
1.1	June 10, 2024	Alex Fhermaye		Updated and Corrected submission
1.2	June 10, 2024	Alex Fhermaye		Template converted to PCI Compliance Policy

Citations

Payment card industry (PCI) compliance policy. Administrative Services Gateway - University at Buffalo. (2021, January 13). https://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/pci-compliance.html

PCI compliance policy. (n.d.-f). https://case.edu/treasurer/sites/case.edu.treasurer/files/2020-01/PCI compliance policy_1.pdf