Payment Card Industry (PCI) Policy Manual

Network and Computer Services

Forward

This policy manual outlines acceptable use Black Hills State University (BHSU) or "University" herein, Information Technology (IT) Network and Computer Services (NCS) and applies to students, faculty, staff, visitors, guests, affiliated campus organizations or non-profit groups, and other individuals, groups and organizations relying on the Black Hills State University as a host through contractual relationships (users). BHSU operates under the governing control of South Dakota Board of Regents (SDBOR). All policies in this manual are superseded by South Dakota Codified Law and SDBOR policies. Should you have any questions regarding use of IT systems, please contact NCS.

Table of Contents

07-100. Compliance with Payment Card Industry (PCI) Policy

Introduction

The payment card industry (PCI) denotes the debit, credit, prepaid, e-purse, ATM (Automated Teller Machine), and POS (Point of Sale) cards and associated businesses. The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures. PCI DSS comprises a minimum set of requirements for protecting cardholder data.

Definitions

Access Control: Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.

Card Verification Code or Value: Data element on a card's magnetic stripe that uses a secure cryptographic process to protect data integrity on the stripe and reveals any alteration or counterfeiting (referred to as CAV, CVC, CVV or CSC, depending on payment card)

- CVC – Card Validation Code (MasterCard payment cards)
- CVV – Card Verification Value (Visa and Discover payment cards)
- CSC – Card Security Code (American Express)

Cardholder Data: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number (PAN), name, expiry date, and card verification value 2 (CVV2) are included in this definition.

Cardholder Data Environment: Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder

data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.

Data: Pieces of information from which understandable information is derived. Data are a collection of information or facts usually gathered as the result of experience, observation, experiment or processes within a computer system or premises. Data may consist of numbers, words or images, particularly as measurements or observations of a set of variables. Data are often viewed as the lowest level of abstraction from which information and knowledge are derived.

Database: Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.

Degaussing: Also called disk degaussing, it is the process or technique that demagnetizes the disk so that all data stored on the disk are permanently destroyed.

Disk Encryption: Technique or technology (either software or hardware) for encrypting all stored data on a device (e.g., hard disk, flash drive). Alternatively, File-Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.

eCommerce: Business transactions over electronic means. This normally means the internet, but can include any electronic interaction – including automated phone banks, touch screen kiosks, or even ATMs. Transactions can include debit/credit cards, but also include any electronic transfer of funds via ACH.

Encryption: Process of converting information into a form only intelligible to holders of a specific cryptographic key. The use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

Full Magnetic Stripe Data: Also referred to as track data. Data encoded in the magnetic stripe or chip is used for authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.

Primary Account Number (PAN): Acronym for primary account number and also referred to as account number. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Removable Electronic Media: Media that store digitized data and can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.

Sanitization: Process for deleting sensitive data from a file, device or system; or for rendering data useless if accessed in an attack

Secure Wipe: Also called secure delete, a program utility used to delete specific files permanently from a computer system

Sensitive Authentication Data: Security-related information (card validation codes/values, full magnetic-stripe data, PINs and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form

Service Code: Three-digit or four-digit value in magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange or identifying usage restrictions.

System Components: Any network component, server or application included in or connected to the cardholder data environment

Types of Data: Data may be in electronic media or in hardcopy format. The following is a list of where data and, specifically, cardholder data may reside:

Electronic Media: Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment and various others.

- Hard drives
- Tapes/media
- CDs
- DVDs
- Compact flash drives, SD
- Dynamic Random Access Memory (DRAM)
- Read Only Memory (ROM and the different variations thereof)
- Random Access Memory (RAM)
- Flash cards
- USB drives, removable media, memory sticks

Hardcopy Format: Hard copy media are physical representations of information. Paper printouts, printers, facsimile ribbons, drums and platens are all examples of hardcopy media.

- Paper receipts or other supporting hardcopy documents and receipts
- Credit card printouts from processing machines
- Invoices
- Purchase orders
- Off-line hard copy batch printouts
- Other hardcopy formats as identified by organizations

07-100.1. Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER:	07-100.1
OFFICE OF RECORD:	Network and Computer Services
ISSUED BY:	Director of Network and Computer Services
APPROVED BY:	Dr. Kay Schallenkamp, President
EFFECTIVE DATE:	October 17, 2012
REVIEWED DATE:	February 14, 2013
REPLACES:	N/A

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University has established a formal policy and supporting procedures regarding PCI Security Policies. This policy shall be reviewed by the NCS director or designee on an annual basis for compliance and for ensuring its adequacy and relevancy regarding the University's needs and goals.

Scope

This policy applies to all Black Hills State University PCI DSS related security policies.

Policy

Black Hills State University shall publish all PCI DSS related policies on the BHSU web site. The policies shall also be disseminated to all relevant vendors, contractors, and business partners.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.

07-100.2. Credit Card Processing (PCI DSS)

NUMBER: 07-100.2
OFFICE OF RECORD: Network and Computer Services
ISSUED BY: Director of Network and Computer Services
APPROVED BY: Dr. Kay Schallenkamp, President
EFFECTIVE DATE: November 11, 2012
REVIEWED DATE: February 14, 2013
REPLACES: October 17, 2012

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University (BHSU) has established a formal policy for credit card processing. This policy shall be reviewed for content and compliance by the NCS director or designee on an annual basis.

Scope

This policy applies to all systems that are subject to PCI DSS requirements.

Policy

- BHSU employees who receive credit card information on paper shall process the transaction immediately. As soon as the transaction has been processed, the credit card information shall be destroyed by shredding through a cross-cut shredder.
- Credit card transactions shall not be conducted via e-mail or other unsecured communication methods (chat, instant messaging, voicemail, etc.) nor stored on any form of media such as a computer, flash drive, external hard-drive, etc. (including scanned images).
- If an employee receives an email or other unsecured communication with cardholder data, that employee must delete the message immediately. The employee must then contact the sender to inform them that the transaction cannot be processed and to provide an alternative means to complete their transaction.
- If it is necessary for staff to accept credit card information over the phone, the information is to be written on a piece of paper and hand-delivered to the appropriate office for processing. The paper containing the credit card information shall be held in secure storage until the transaction is verified. It

shall then continue to be held in secure storage until it is shredded on a cross-cut shredder.

- Credit card information may be faxed to an office. However, the fax machine must be in a secure area. Faxed information must be immediately hand delivered to the appropriate office for processing. Any electronic memory on fax/scanning machines used to disseminate credit card information must be fully erased or physically destroyed when the equipment is retired.
- All forms shall be designed so that any credit card information can be easily cut off and shredded after processing.
- Any forms containing cardholder information must be held in secure storage, until the transaction is verified, and then it shall be shredded on a cross-cut shredder.
- Terminals and underlying applications must be configured to mask the PAN when displayed.
- The security code shall not be requested for any transaction unless through an authorized third party service provider.
- All terminals and underlying systems must be configured to truncate account numbers on printed copies of receipts.
- Recurring payments shall be handled by the credit card service provider and will not require access to the PAN by BHSU employees.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.

Revision History

1.1 17 October 2012
1.2 30 November 2012 (Clarified electronic cardholder data transaction)

07-100.3. Credit Cardholder Data Access Control in Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER:	07-100.3
OFFICE OF RECORD:	Network and Computer Services
ISSUED BY:	Director of Network and Computer Services
APPROVED BY:	Dr. Kay Schallenkamp, President
EFFECTIVE DATE:	October 17, 2012
REVIEWED DATE:	February 14, 2013
REPLACES:	October 17, 2012

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University has established a formal policy and supporting procedures regarding cardholder data access control. This policy shall be reviewed for content and compliance by the NCS director or designee on an annual basis.

Scope

This policy applies to all systems in the cardholder data environment.

Policy

Black Hills State University shall protect cardholder data by ensuring the following access controls are in place in the cardholder data environment:

- Access rights for privileged users are restricted to the fewest privileges necessary to perform job responsibilities
- Privileges are assigned to individuals based on job classification and function, such as Role-Based Access Control (RBAC)
- An e-mail process is utilized to request access to cardholder. This request must specify the privileges requested and the duration of the request. The message must be submitted to the Director of Network and Computer Services by the individual's supervisor.
- Access controls are implemented via an automated access control system
- Access control systems are in place on all system components
- Access control systems are configured to enforce privileges assigned to individuals based on job classification and function

- Access control systems have a deny all setting

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.

07-100.4. Authorizing Third Party Service Providers in Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER:	07-100.4
OFFICE OF RECORD:	Network and Computer Services
ISSUED BY:	Director of Network and Computer Services
APPROVED BY:	Dr. Kay Schallenkamp, President
EFFECTIVE DATE:	October 17, 2012
REVIEWED DATE:	February 14, 2013
REPLACES:	N/A

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University has established formal procedures regarding the addition of an authorized third party service provider. This policy shall be reviewed for content and compliance by the NCS director or designee on an annual basis.

Scope

This policy applies to the addition of any third party service provider to the list of authorized service providers.

Policy

To add a new Service Provider, a department must:

1. Discuss the reasons for adding the Service Provider with the Controller or Vice President for Finance and Administration.
2. The credentials of the Service Provider must be researched. To be considered, the Service Provider should be a Level 1 processer and be named on the list of processors approved by Visa and MasterCard.
3. Obtain a copy of the proposed contract from the Service Provider.
4. Submit the contract to the Controller and Vice President for Finance and Administration.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.

07-100.5. Use of Employee Facing Technologies in Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER:	07-100.5
OFFICE OF RECORD:	Network and Computer Services
ISSUED BY:	Director of Network and Computer Services
APPROVED BY:	Dr. Kay Schallenkamp, President
EFFECTIVE DATE:	October 17, 2012
REVIEWED DATE:	February 14, 2013
REPLACES:	N/A

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University (BHSU) has established a formal policy and supporting procedures regarding the use of employee facing technologies. This policy shall be reviewed for content and compliance by the NCS director or designee on an annual basis.

Scope

This policy applies to all BHSU employees facing mobile technology used in the cardholder data environment. Employees facing mobile technologies are system components and additional IT resources deemed critical by Black Hills State University. Some examples of employee facing technologies are:

- Remote access technologies
- Wireless technologies
- Removable electronic media
- Laptops
- Personal Data Assistants (PDA)
- Cell phone

For definitions of certain terms see the Compliance with Payment Card Industry Data Security Standards (PCI DSS) policy document.

Policy

BHSU will ensure that the usage policies for critical employee facing technologies shall adhere to the following conditions for purposes of complying with the Payment Card

Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council 2009):

- BHSU shall require explicit management approval to use the technologies.
- BHSU shall require all technology use be authenticated with user ID and password or other authentication item.
- BHSU maintains a list of all devices.
- BHSU shall require acceptable uses for the technology.
- BHSU shall require acceptable network locations for the technology.
- BHSU shall require a list of company-approved products.
- BHSU shall require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.
- BHSU shall require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.
- BHSU shall prohibit copying, moving or storage of cardholder data onto local hard drives or removable electronic media when accessing such data via remote-access technologies.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.

07-100.6. Information Security Responsibilities Related to Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER:	07-100.6
OFFICE OF RECORD:	Network and Computer Services
ISSUED BY:	Director of Network and Computer Services
APPROVED BY:	Dr. Kay Schallenkamp, President
EFFECTIVE DATE:	October 17, 2012
REVIEWED DATE:	February 14, 2013
REPLACES:	N/A

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University (BHSU) has established a formal policy and supporting procedures regarding Information Security Responsibilities. This policy shall be reviewed for content and compliance by the NCS director or designee on an annual basis.

Scope

This policy applies to all employees and contractors who have access to the BHSU cardholder data environment.

Policy

BHSU shall ensure that the Information Security Responsibilities policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council 2009):

- Formal assignment of information security is to be given to the BHSU Chief Information Officer (CIO) and Director of Network and Computer Services.
- The responsibility for creating and distributing security policies and procedures is to be formally assigned to the CIO and Director of Network and Computer Services.
- The responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business

unit management personnel is to be formally assigned to the Network and Computer Services Network Security Officer.

- The responsibility for creating and distributing security incident response and escalation procedures is to be formally assigned to the BHSU Network Security Officer.
- The responsibility for administering user account and authentication management is to be formally assigned to the Director of BHSU Network and Computer Services.
- The responsibility for monitoring and controlling all access to cardholder data is to be formally assigned to the Controller.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.

07-100.7. Vulnerability Scans in Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER:	07-100.7
OFFICE OF RECORD:	Network and Computer Services
ISSUED BY:	Director of Network and Computer Services
APPROVED BY:	Dr. Kay Schallenkamp, President
EFFECTIVE DATE:	October 17, 2012
REVIEWED DATE:	February 14, 2013
REPLACES:	N/A

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Black Hills State University (BHSU) has established a formal policy for conducting vulnerability scans. This policy shall be reviewed for content and compliance by the NCS director or designee on an annual basis.

Scope

This policy applies to all systems that are subject PCI DSS requirements.

Policy

BHSU shall conduct quarterly internal/external vulnerability scans for all hosts in the campus cardholder data environment. Audited external scans will be performed by an authorized third party. Internal scans shall be performed by the BHSU Infrastructure Security Manager or designee. Logs of the quarterly internal/external scans shall be provided to the Director of Network and Computer Services.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see the Employee Handbook for guidelines.