SOUTH DAKOTA SCHOOL OF MINES AND TECHNOLOGY

Policy Manual

SUBJECT: Compliance with Payment Card Industry Data Security Standards (PCI DSS)

NUMBER: Policy 8-4 (formerly Policy VIII-04)

REVISED: August 2022

POLICY

South Dakota Mines will publish all PCI DSS related policies on the Mines web site. The policies will also be disseminated to all relevant vendors, contractors, and business partners.

PURPOSE

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Mines has established a formal policy and supporting procedures regarding PCI Security Policies. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the University's needs and goals.

SCOPE AND DEFINITIONS

This policy applies to all Mines PCI DSS related security policies.

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 that uses a secure cryptographic process to protect data integrity 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 on the card 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
- Mobile devices

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

SOURCE: Information Technology Services Nov. 6, 2012, May 2013, August 2022