SNOW COLLEGE

Policy # 202
Date Approved: January 22, 2013
Date Amended: May 2020
Responsible Office: Controller's Office

SUBJECT: PAYMENT CARD HANDLING POLICY

1.0 PURPOSE

1.1. The purpose of this policy is to protect payment card data and to comply with the Payment Card Industry Data Security Standards (PCI DSS) requirements for transmitting, handling, and storage of payment card data.

2.0 REFERENCES

2.1. Payment Card Industry Data Security Standard (PCI DSS), Requirements and Security Assessment Procedures, https://www.pcisecuritystandards.org/pci_security/

3.0 DEFINITIONS

3.1. **CAV2, CVC2, CID, or CVVC data:** The three or four-digit value printed on the card or signature strip used to verify card-not-present transactions.

3.2. **Degaussing**: Process or technique that demagnetizes the disk such that all data stored on the disk is permanently destroyed.

3.3. **Cardholder data**: Cardholder Data includes the Primary Account Number (PAN), Cardholder Name, Expiration Date, and Service Code.

3.4. **E-Commerce**: Electronic commerce consists of the buying and selling of products or services over electronic systems such as the Internet or other computer networks.

3.5. **Mask** (or truncate): The practice of removing a data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits while replacing the deleted numbers with asterisks (*).

3.6. **Media**: Objects on which data can be stored. These include computers, removable electronic media, networking and communications hardware, telecommunications lines, paper receipts, paper reports, and faxes.

3.7. **Payment Card**: An instrument used in lieu of cash in the form of a credit, debit, or charge card.

3.8. **Payment Card Industry Data Security Standards (PCI DSS)**: Data security standards developed by the major payment card companies (Visa, MasterCard, Discover, American Express and JCB) to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

3.9. **Payment Application Data Security Standards (PA DSS)**: Data security standards derived from PCI DSS as a guideline for software vendors and other developed secure payment applications that do not store sensitive authentication data, and ensure their payment applications support compliance with the PCI DSS.

3.10. **Payment Card Merchant**: A department or other auxiliary which has been set up through a financial institution with the ability to accept payment cards as payment for goods or services.

3.11. **Payment Gateway**: Facilitates the transfer of payment card transaction information between a payment portal (such as a website) and the acquiring bank.

3.12. **PCI Compliance Committee**: Committee comprised of employees from the College's Information Technology (IT) Department, Information Security Officer (ISO), and Controller's Office charged with ensuring the College's compliance with PCI DSS.

3.13. **Primary Account Number (PAN)**: Unique payment card number that identifies the issuer and the particular cardholder account.

3.14. **Point of Sale (POS) device**: A POS device is the hardware and/or software used to process payments and transactions at merchant locations.

3.15. **Sensitive Authentication Data**: Sensitive Authentication Data includes the full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

4.0 POLICY

4.1. All departments and other auxiliaries within the College that function as a payment card merchant must comply with established security control measures including:

4.1.1. Approval from the College Controller (unless the Controller is the chair of the PCI Compliance Committee) and PCI Compliance Committee before entering into any contract or purchase of software and/or equipment that involve payment cards. This requirement applies regardless of the transaction method or technology used.

4.1.2. Notification to the Controller's Office and Information Security Officer of all technology implementations.

4.1.3. Establishment of payment card handling procedures for safeguarding cardholder data. This pertains to ALL transactions initiated via the telephone, in person, mail order, ecommerce, etc.

4.1.4. Compliance with current Payment Card Industry Data Security Standards (PCI DSS).

4.1.5. Participation in an annual security Self-Assessment Questionnaire (SAQ) conducted by the Payment Card Merchant in conjunction with the PCI Compliance Committee and reported to the Vice President of Finance and Administrative Services to ensure compliance with this policy and associated procedures.

4.1.6. Payment applications and POS devices implemented must be PA DSS validated.

4.2. All ecommerce payments must be processed through a College approved payment gateway, unless an exemption has been approved by the PCI Compliance Committee.

4.2.2. A department or other auxiliary of the College shall not enter into an outsourcing agreement with a third-party provider, including software applications, for payment card processing until such an agreement is first approved by the Controller in conjunction with the PCI Compliance Committee and the Procurement Office.

4.3. All cardholder data and customer information must be kept secure and confidential at all times.

4.3.2. Payment card receipts should be treated in the same manner as cash. Refer to the College's Cash Handling Policy.

4.3.3. All media containing cardholder data must be maintained in a secure environment limited to authorized staff. Secure environments include locked drawers, file cabinets in locked offices, safes, and encrypted electronic storage devices.

4.3.3.1. Payment card merchants who accept mail or phone payments must immediately destroy any paper notes that contain any Cardholder Data once the transaction is completed. e.g. cross-cut shredding.

4.3.4. Sensitive authentication data must never be stored on computers or networks.

4.3.5. The PAN and expiration date must be truncated, masked, or encrypted wherever it is electronically stored.

4.3.6. Cardholder data must be transmitted or delivered in a secured manner, such as SSL encryption, or sealed envelopes through the US postal service or equivalent.

4.3.7. Cardholder data must never be sent or accepted via end-user messaging technologies (for example: fax, email, instant messaging, SMS, chat, etc.) or over voicemail. If inadvertently received, the cardholder data must never be used to process a payment. Follow approved departmental operating procedures for the appropriate method of responding to and deleting the cardholder data if received from a payee in a prohibited manner.

4.3.8. Cardholder data must not be stored in spreadsheets, word processing documents, personal databases, text files, or other types of data storage mechanisms.

4.3.9. The payment card merchant must use processing equipment that produces receipts with a masked (or truncated) cardholder's PAN. Payment card merchants must mask the cardholder's PAN on the customer's receipt and should also mask the merchant's copy of the receipt if there is no business constraint.

4.3.10. The level of security controls applied to the College's network must at least match the highest level of classification of the data being transmitted.

4.3.11. All personnel involved in payment card handling are required to receive payment card handling security training at least annually provided by the PCI Compliance Committee.

4.4. All cardholder data and customer information must be protected from unauthorized access.

4.4.2. Physical and electronic access to payment card processing and cardholder data must be restricted to appropriate and approved personnel.

4.4.3. Background checks must be performed in accordance with current Human Resource policy. https://snow.edu/offices/hr/

4.4.4. Appropriate segregation of duties must be established between payment card processing (including refunds) and the reconciliation function. Proper approval, as determined by each Payment Card Merchant, of all payment card refunds is required.

4.4.5. The Controller's Office and Information Security Officer must be notified prior to implementation of any technology changes affecting payment card transaction processing associated with the merchant account.

4.4.6. Proper user authentication and password management must be in place as required by PCI DSS and the College Information Security Policy.

4.4.7. All access to cardholder data must be logged and monitored.

4.5. All breaches in security regarding cardholder data must be reported to the Vice President of Finance and Administrative Services, the Chief Information Officer and the Information Security Officer immediately upon discovery.

4.6. Self-assessments and testing must be performed to ensure compliance with PCI DSS.

4.6.2. Payment card handling procedures and equipment are subject to audit by the College Internal Audit department, external audit, or Payment Card review firms.

4.6.3. An annual PCI DSS self-assessment and periodic network-based vulnerability scans must be conducted to ensure security controls are in place to protect the technology implementations.

4.6.4. The results of the annual self-assessment must be reported to the Vice President of Finance and Administrative Services and the Controller's Office and Information Security Officer.

4.6.5. Departments not complying with approved safeguarding, storage, and processing procedures may lose the privilege to serve as a payment card merchant.

4.7. Payment card transaction records and cardholder data must be retained and destroyed appropriately.

4.7.2. Original sales receipts and all supporting documentation must be retained as established by the Utah Code Section 63A- 12 or State Agency General Records Retention Schedule.

4.7.2.1. All paper documentation containing cardholder data must be destroyed in a manner that will render it unreadable, e.g. cross- cut shredding.

4.7.2.2. All electronic cardholder data must be rendered unreadable by destroying the media on which it is stored, e.g. drilling holes in the media or when cost-effective degaussing.

4.8. Payment Card Merchants with Payment Cards that have been inadvertently left and remain unclaimed:

4.8.2. May return a Payment Card inadvertently left at their location, to the Cardholder, until the close of the business day. A Payment Card may only be returned to the cardholder if positive identification is provided.

4.8.2.1. A Payment Card not claimed by the cardholder by the close of the business day must be processed in accordance with the applicable merchant agreement (e.g. following the lost Payment Card instructions on the back of a Payment Card or send the Payment Card to the College Cashier's Office to be placed in the vault until claimed).