BLACK HILLS STATE UNIVERSITY

Policy and Procedure Manual

SUBJECT: Credit Card Payments

NUMBER: 7:1

Office: Network and Computer Services

Source: Payment Card Industry (PCI) Data Security Standards (DSS)

Link: https://www.pcisecuritystandards.org/security_standards/index.php

---

1. Purpose

   This policy provides guidance for University departments currently accepting credit card payments for goods or services for deposit to University accounts in compliance with the Payment Card Industry ("PCI") Data Security Standards ("DSS").

2. Definitions

   Card Holder Data ("CHD"): refers to a cardholder's card number, expiration date, PIN, and the three or four-digit CAV2/CVC2/CVV2/CID number on the back of the credit card.

3. Policy

   a. University employees are required to comply with all applicable laws, rules, regulations, and policies pertaining to the acceptance of credit card payments for goods or services at the University, including those standards set by the PCI.

   b. All University employees involved in the collection, processing, storage, or transmission of CHD are required to participate in PCI Awareness Training as provided by the University prior to their handling of CHD.

      i. Student employees at the University who handle the processing of more than one (1) credit card transaction at a time (i.e., bulk transactions) must

have a background check conducted and participate in PCI Awareness Training as provided by the University prior to their handling of CHD.

c. The physical location of all credit card terminals at the University must be approved by the University's PCI Compliance Officer or designee.
d. No agreement or contract associated with the collection, storage, processing, or transmission of CHD shall be entered into without the review and approval of the University's PCI Compliance Officer or designee. This includes the handling of credit card processing through third parties.
e. Access to credit card information at the University shall be limited to departmental employees on a "need-to-know" basis. Unauthorized personnel shall not be permitted access to CHD.

4. Procedures
    a. All departments at the University who process CHD must document specific departmental procedures for the collection and processing of CHD. These procedures must be on file with the University's PCI Compliance Officer or designee and must include, not exclusively, the following:
        i. Steps to process CHD received in person, by mail, by telephone, and/or via electronic communications in adherence with this policy;
        ii. A 'start of day' process including instructions that all credit card terminals should be checked to ensure the tamper-resistant seal on the bottom of the terminal is intact, documented as being so; and
        iii. An 'end of day' process including an instruction that credit card terminals shall be batched out each day.
    b. Collection of CHD
        i. The collection of CHD using an electronic fax machine is discouraged but permitted at the University.
            1. The fax machine must be accessible to departmental staff only.
            2. Departments accepting CHD via fax cannot use the option that converts faxes to electronic documents.

ii. The collection of CHD over the telephone or through the mail is discouraged but permitted at the University if all other procedures are followed as set forth in this policy.

iii. The collection of CHD through electronic mail (email) is not permitted at the University.

1. In the event that CHD is delivered via email, individuals must immediately notify the University's PCI Compliance Officer or designee, with the circumstances of the email: date, time, from address, to address, and subject line. In the body, include the last four digits of the CC number involved– format (i.e., XXXXXXXXXXXX1234). The email containing the CHD must not be forwarded during this notification process.
2. Following notification to the University's PCI Compliance Officer, individuals must delete the email message by highlighting the email message in Outlook and using 'shift+delete' with confirmation, or by deleting the email message and then immediately emptying their 'deleted items' folder.
3. The credit card payment must not be processed from the email. Instead, the individual must contact the donor/customer directly via telephone or email (do not reply to the original email, but create a new email message) and indicate the University cannot accept CHD via email and request the information be provided over the phone.

c. Storage of CHD

i. Electronic storage of credit card information is not permitted at the University under any circumstances.

ii. Temporary physical storage of CHD is permitted at the University, provided that any document containing CHD is stored in a locked cabinet/file for a maximum of two (2) business days. If it is necessary to store documents with CHD for more than two (2) business days,

individuals must receive approval from the University's PCI Compliance Officer or designee.

iii. Permanent physical storage of CHD is not permitted. CHD on documents or forms must be destroyed using a crosscut or micro shredder. Destroying the information with a strip shredder is not sufficient.

d. The transportation of CHD from one place to another for any reason shall be limited to employees who have regular access to the CHD. The transportation must occur in a secure, locked device.

e. All in-person, telephone, mail, and fax credit card payments at the University shall use any device approved by the University's PCI Compliance Officer or designee.

f. All online/e-commerce credit card payments at the University shall be processed using any service approved by the University's PCI Compliance Officer or designee.

5. Responsible Administrator

The VP for Finance & Administration, or designee, is responsible for the ad hoc and annual review of this policy and its procedures. The University President is responsible for approval of this policy.

SOURCE: Adopted by President 9/7/2021. Reviewed 2023.07.10 Reviewed 2024.10.22