

Office/Contact: Accounts Receivable

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

Link: [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php)

---

**SOUTH DAKOTA STATE UNIVERSITY**  
**Policy and Procedure Manual**

SUBJECT: Credit Card Payments

NUMBER: 5:20

---

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

- iii. An 'end of day' process including an instruction that credit card terminals shall be batched out each day.
- d. The physical location of all credit card terminals at the University must be approved by the University's PCI Compliance Officer, successor, or designee.
- e. 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, successor, or designee. This includes the handling of credit card processing through third parties.
- f. Access to credit card information at the University shall be limited to departmental employees on a "need-to-know" basis. Unauthorized personnel, including custodial staff, shall not be permitted access to CHD.
- g. Collection of CHD
  - i. 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. Collection of CHD over the telephone or through mail is discouraged, but permitted at the University if all other procedures are followed as set forth in this policy.
  - iii. Collection of CHD through electronic mail (e-mail) is not permitted at the University.
    - 1. In the event that CHD is delivered via e-mail, 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 4 digits of the CC number involved- format (ie. XXXXXXXXXXXXX1234). 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 e-mail message by highlighting the e-mail message in Outlook and using 'shift+delete' with confirmation, or by deleting the e-mail message and then immediately emptying their 'deleted items' folder.

and request the information is provided over the telephone.

h. Storage of CHD

i. Elec