This document contains procedures established for Wichita State University departments currently accepting credit card payments for goods or services for deposit to State of Kansas accounts. All procedures set forth below comply and support the Security of Credit Card Data Policy in WSU Policies and Procedures, Section 13.14. *Card Holder Data (CHD) refers to a cardholder’s card number, expiration date, PIN and the 3/4 digit CAV2/CVC2/CVV2/CID number on the back of the card. Each department maintains their own specific inter-office procedures that build upon, but do not contradict this document.

Receiving CHD

- Receiving CHD will only occur on machines designated specifically for the purpose of collecting CHD. Those machines will only be connected to approved network jacks, and will be physically locked into the approved jacks.
- Receiving CHD over the phone or through mail is discouraged, but permitted, if all other procedures are followed as set forth in this document.
- Receiving CHD using an electronic fax machine is discouraged, but permitted.
  - The fax machine should be accessible to departmental staff only.
  - Faxes with CHD should print only when departmental staff are available to pick up fax page. (i.e. Use fax option that requires a code to print).
  - Departments accepting CHD via fax cannot use the option that converts faxes to electronic documents.
  - The fax machine must be a stand-alone device, not network-connected or part of a multi-function printer.
- Receiving CHD through any unsecure messaging (chat, text, Facebook, etc.) is NOT permitted.
- Receiving CHD through electronic mail (email) is NOT permitted. In the event that CHD is delivered via email:
  1. Notify creditcards@wichita.edu 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 i.e. XXXXXXXX1234.
  2. Permanently delete the email by highlighting the email and then doing a “Shift+delete” with confirmation (or delete the email and then empty your 'deleted items' folder).
  3. Do NOT process the credit card payment from the email.
  4. Contact the donor/customer directly via phone or email (do not reply to original email, but create a new email message). Indicate that we CANNOT accept CHD via email, and request that they provide the number over the phone.
Access to CHD

- Access to credit card information should be limited to department employees on a “need-to-know” basis.
- Access to payment system must be approved and granted by departmental PCI contact and payment system administration.
- Custodian staff (or other unauthorized personnel) should have no access to CHD.
- All employees involved in collection, processing, storage or transmission of CHD are required to participate in an annual PCI Awareness Program and the mandatory FERPA training course per WSU policy.
- Student employees who handle the processing of more than one credit card transaction at a time (bulk) must have a background check conducted.
- All employees processing CHD must use their assigned, unique user id when handling CHD.
- A list of all personnel and devices that store, process, or transmit credit card data must be provided to Financial Operations. They must be updated as changes occur.
- Access to CHD must be immediately removed upon employee termination.
- Transportation of CHD from one place to another for any reason:
  - Should be limited to employees who have regular access to the CHD.
  - Should be in a secure, locked bag.
- Remote access to the systems that process CHD is limited to authorized personnel, and only from authorized work stations. There is no remote access into the CHD from outside the CHD. Each system has an “always on” encrypted connection to the remote access server. Any user accessing the station remotely is prohibited from copying, moving, or storing any CHD onto local hard drives or removable media. All CHD must be protected in accordance with PCI DSS requirements.

Storage of CHD

- **Electronic storage** of credit card information is not permitted under any circumstances.
- **Temporary physical storage**
  - Any document containing CHD must be stored in a locked cabinet/file for a maximum of two business days. If it is necessary to store documents with CHD more than two business days, Financial Operations approval is necessary.
- **Permanent physical storage** of CHD is not permitted.
  - CHD on documents or forms must be destroyed using a cross-cut or micro shredder. Destroying with a strip shredder is not sufficient.
  - Forms with credit card numbers should NOT be put into a shredder bin to be shredded at another location.

Processing CHD

- All departments processing CHD must **document specific departmental procedures** for collecting and processing the CHD. Each set of specific procedures for a department will be stored with the PCI Committee. Any changes to the department procedures should be sent to them immediately. Including, but not limited to, the following:
Campus Departments – Credit Card Procedures

- Steps to process CHD received in person, by mail, by phone, by fax and/or via e-commerce.
- Each payment station should be used only for the express purpose of processing credit cards.
- “Start of Day” Process
  - All credit card terminals should be checked to ensure the tamper resistant seal on the bottom of the terminal is intact and serial number on device matches the device that was issued to the department.
- “End of Day” Process
  - Payment stations (PC only) should not be turned off unless instructed by Financial Operations.
- Campus Departments using Cashiering Merchant Edition (CME)
  - Drawers shall be closed and balanced at the end of each business day.
  - Sign off of CME
  - The physical location of the credit card terminal must be approved by Financial Operations personnel and placed in a secure location when office personnel are not present.
  - A sales receipt must be offered to the customer containing the department’s refund policy.

- All in-person, phone, mail, fax payments should use *TouchNet, Inc.’s Cashiering (CME) or Marketplace software applications.
- All online/e-commerce payments should be processed using *TouchNet, Inc.’s Marketplace application, unless an exception has been made on a case-by-case basis.
- Any software/hardware used to collect, access, process or transmit CHD must be reviewed and approved by Financial Operations. Financial Operations will maintain the list of software/hardware approved for use by WSU departments.
- No agreement or contract associated with the collection, storage, processing or transmission of CHD shall be entered into without the review and approval of Financial Operations. This includes the handling of credit card processing through 3rd parties.

Security Incident – Suspected/Confirmed Credit Card Breach

It is required that each department has a copy of the “Credit Card Security Incident Response Plan” posted with their “Inter-Office Credit Card Procedures”. Refer to that document for the steps to take during a suspected or confirmed credit card breach. For a copy of the “Credit Card Security Incident Response Plan”, please either contact Accounts Receivable at x3070 or visit their website at http://wichita.edu/ccrdpymts.

*TouchNet, Inc. is Wichita State University’s preferred software vendor for all WSU credit card processing needs. If your department is using any other software or service to process credit card payments, it must be approved by Financial Operations. Please contact creditcards@wichita.edu for all questions regarding credit cards for Wichita State University.
# Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Person</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/07/08</td>
<td>Blaine Linehan</td>
<td>Created document from old version.</td>
</tr>
</tbody>
</table>