Payment Card Control and Security Procedures for Cardholder Data (CHD) (as defined in Policy 2110)

November 2017

**ACCEPTANCE:**

- **DO** accept CHD through an online process approved by Fiscal Services and IT Security
- **DO** accept CHD on a payment card reader approved by Fiscal Services
- **DO** accept CHD on an authorization form sent through a stand-alone fax machine in a secure location
- **DO** accept CHD on an authorization form sent through the U.S. Mail
- **DO** accept CHD on the phone, **only** if direct entry into approved POS device **and** by authorized staff who have completed PCI DSS training*
- **DO** permit access to CHD **only** for employees with legitimate need-to-know
- **DO** accept CHD **only** on active readers reported on the PCI Council’s Approved PTS Device List
- **DO** accept CHD **only** thru payment applications that comply with the PA-DSS
- **DO** ensure PCI DSS compliance of service providers with whom CHD is shared, or that could affect CHD security
- **DON’T** accept CHD by email
- **DON’T** accept CHD as an attachment to an email
- **DON’T** type CHD on a computer keyboard or laptop
- **DON’T** accept CHD on a fax machine located in an unsecure area or connected to the network
- **DON’T** send CHD through campus mail
- **DON’T** accept CHD on voice mail; direct callers not to leave card info on recorded message
- **DON’T** retain card validation code/value printed on the card (CVC2, CVV2, CID). **If** collecting for card verification purposes, it must be destroyed once the transaction is authorized
- **DON’T** direct customer to a specific computer or location to pay (can say “choose any internet-enabled device”)
- **DON’T** input CHD into an e-commerce platform on customer’s behalf

**STORAGE:**

- **DO** keep paper CHD locked in a safe or secure filing cabinet until processed
- **DON’T** store CHD using any electronic method, including database, secure file or spreadsheet
- **DON’T** leave unprocessed CHD in an unsecure location

**DISPOSAL:**

- **DO** properly destroy CHD: **immediately** after processing, use a cross-cut shredder or small hole punch
- **DON’T** dispose of CHD in any other way

**ARCHIVING THE TRANSACTION RECORD – NO CHD PRESENT:**

- **DO** store the last 4 digits of the card number, signature, transaction ID and dollar amount for the record retention period (3 years after fiscal year for Banner orgs and 10 years for funds)

I certify that I have read these guidelines and will process all payment cards in accordance with them.

<table>
<thead>
<tr>
<th>Printed Name</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
</table>

*This form must be retained in the department and renewed on an annual basis.*

*Annual Campus Guard PCI DSS training coordinated through Fiscal Services*