CREDIT CARD INFORMATION:
UNIVERSITY POLICY ON CARDHOLDER SECURITY

Overview:

Bradley University accepts credit card payments for various operations on campus. To facilitate this, the University has become a merchant with several locations on campus that have their own credit card terminal to process the charges. Other departments rely on the Cashiers in the Controller’s Office to process the charges. Still other departments utilize payment processing software. The University has contracted with Wells Fargo Merchant Services to process the charges and remit payment to its bank. Wells Fargo requires all of its merchants and their service providers to comply with recent Visa and MasterCard security requirements (Payment Card Industry Data Security Standards).

The PCI Data Security Requirements apply to all merchants that store, process or transmit cardholder data. Merchants are required to protect their business, customer (cardholder) and the integrity of the payment system by complying with requirements governing the safekeeping of account information. With respect to the storage of cardholder information, merchants are not allowed to store the following under any circumstance:

- Full contents of any track from the magnetic stripe on the back of the card
- Card-validation code (3-4 digit value printed on signature panel on back of card)
- PIN Verification Value (PVV)

All credit card terminals used by the University have recently been updated to comply with the track requirements as well as provide the customer copy with truncated number information. No department on campus should request or receive the card validation code. The University does not accept debit card transactions processed with a PIN number. Thus, the PINN Verification Value (PVV) is never collected or stored.

Merchants can store only that portion of the customer’s account information that is essential to the business – i.e., name, account number or expiration date. All material containing this information must be stored in a secure area limited to authorized personnel. Furthermore, when using agents or third parties (vendors, processors, software providers, payment gateways), the University must ascertain the agent’s compliance with all rules and regulations governing cardholder information security.

Additionally, the PCI Data Security Standards apply to all “system components” which is defined as any network component, server or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including both internal and external (web) applications.
The Office of Information Resources and Technology takes primary responsibility for ensuring the PCI Security Requirements for all system components. The Controller’s Office and the various departments on campus who process credit card payments are responsible for physically securing and storing cardholder information, including certain aspects of the transmission of cardholder information. This document serves as policy for these latter functions.

**Cardholder Information Access:**

To be allowed to accept credit card payments, the University department must adhere to the following:

1) Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunications lines, paper receipts, paper reports and faxes) that contain cardholder information.

2) Limit credit card processing to key individuals who acknowledge in writing they have read and understand the University’s security and procedures.

3) Keep cardholder information storage to a minimum. The following data retention procedures apply:
   a. Full cardholder information must be kept separate from deposit documentation that requires the 3-7 year retention for IRS, business and legal purposes. Only the truncated number may be attached to this documentation.
   b. Full cardholder name, account number and expiration date can be stored in a locked environment for an 18-month retention period that corresponds with the allowed chargeback period. Access to the locked environment should be limited and a list kept of all key holders.
   c. Disposal of cardholder information after the 18-month period must be by shredding. There should be an automatic process to remove, at least on a quarterly basis, stored cardholder data that exceeds the chargeback retention period of 18 months. Departments may be subject to an audit, at least on a quarterly basis, to verify that stored cardholder data does not exceed the chargeback retention period.
   d. Any manual documentation of credit card information unless used and stored as in (b) above must be shredded immediately after use.
   e. Sensitive authentication data such as the mag-stripe track contents, the 3 to 4 digit CVV/security code, and any PVV information (used with debit cards), must NOT be stored in any way, on any paper or computer media or system, even if encrypted. If any cardholder data is erased, it must be unrecoverable.

**Transmission of Cardholder Information:**

1) Cardholder information must be encrypted during transmission over the internet.

2) Cardholder information must never be sent via unencrypted email. If e-mail is to be used for cardholder information, the information should be sent only in an encrypted attachment or using only a secure e-mail service. You must use an
encryption technology approved by the Office of Information Resources and Technology if you must use e-mail for transmission of cardholder information.

3) If an e-mail is received unrequested with credit card information, the e-mail must be deleted from both the inbox and deleted items folder. Remove all cardholder information before replying to such e-mail.

4) Encryption keys for cardholder information will be managed by the Office of Information Resources and Technology according to documented procedures that meet the requirements of the PCI Data Security Standard.

3rd Party Providers:

1) When engaging agents or third parties (vendors, processors, software providers, payment gateways, web-housing companies), the University must ascertain the agent’s compliance with payment card industry security requirements. Proof of compliance will be required by the University’s PCI DSS Committee and will be kept on file. Contract provisions between the University and the 3rd party must acknowledge that the 3rd party is responsible for security of cardholder data in their possession. Contracts with third parties can be terminated by the University if the third party violates the agreement or PCI compliance.

2) If using a software package that stores, handles or processes cardholder information, the department must ensure that all system components and software have the latest vendor-supplied security patches installed within one month of release.

3) All systems (PC’s, servers, and networks) that process credit card information must be protected by anti-virus, anti-spyware, and other available tools used for protection from malignant software. No wireless access is permitted.

Incident Response: Only individuals who need to access or use cardholder information should do so, and should access only the information needed to perform their job functions. Access of more than the minimum information needed by any University employee is prohibited. If you believe credit card information has been compromised or improperly accessed or used, or if you suspect that any systems or security measures protecting cardholder information have been breached, contact immediately a member of the Credit Card Security Incident Response Team.

I have read and understand the above policy on credit card information security. I agree to comply with the PCI Data Security Standards. I understand that noncompliance may result in deactivation of my merchant account and the imposition of fines if a security breach occurs.

_____________________________________          ________________________
PRINT NAME       Date

_________________________            _______________________
SIGNATURE      DEPARTMENT

TITLE/POSITION
Updated 12/10/2014