Payment Card Acceptance Information and Procedure Guide *(for publication on the Treasury Webpages)*

A companion guide to University policy 6120, Payment Card Acceptance

Standards for Business Processes, Paper and Electronic Processing

The standards that follow are adapted from the credit card industry's "Payment Card Industry Data Security Standards" (PCI DSS). All units must comply with these standards, regardless of what method is used for processing credit cards.

I. Storage and Access to Cardholder Data

A. Keep storage of cardholder data to a minimum. Only information necessary for business processing should be retained. Do not store any cardholder data for longer than six months.

B. Never store the following credit card data elements:

1. Full contents of any track from a Magnetic Stripe

2. CAV2/CVC2/CVV2/CID. These are the three-digit numbers from backs of the cards (see "Card Verification Code or Value" in "Definitions")

3. Personal identification number (PIN)/PIN Block

C. When designing any forms used for credit card sales, locate sensitive cardholder data (see above) together on the form, so that it can be easily removed from the form and shredded.

D. Develop a disposal policy and adhere to it. Verify on a regular basis, at least quarterly, that this policy is functioning correctly.

E. Destroy media properly:

1. Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

2. Render cardholder data on electronic media unrecoverable so that it cannot be reconstructed.

F. Limit access to cardholder data to those individuals with a business need.

G. Maintain a current list of those individuals with access to credit card data.

H. Assign access privileges based on job classification and responsibilities.

I. Review, at least quarterly, all data access controls confirming that there is a business need to allow access of each type.

J. Mask the Primary account number (PAN), showing only the last four digits, anywhere it is stored (this includes all portable devices, logs, backup media, A/P systems, etc.).

K. Physically restrict any credit card processing areas to those individuals who have authority to be there.

L. Do not use unsecured e-mail (such as Broncomail or Google Mail) to transmit cardholder information.

1. Caution: Instruct Customers of this prohibition. Additionally, if a unit receives credit card information via unsecured e-mail, the unit must delete the e-mail, and not process the transaction, notifying the Customer.

a) Store backups in a secure location, preferably off-site, and review the security of the storage facility at least annually, retaining documentation of that review.

b) Identify and manage sensitive information contained on terminals, laptops, and other media devices using appropriate technology tools.

c) Once taken out of production, wipe clean of old transactions any terminals, laptops, and other media devices that are not currently used for processing cardholder data.

Table 1 – *Methods of Processing Transactions*

Method	Description	Sending Transactions t the Bank
PC Processing	Unit must purchase required tools (contact Purchasing). The PC that is processing credit cards must… • Be a stand-alone machine (no Web surfing or other activities permitted) • Connect to the OIT PCI-compliant infrastructure	
Secure Web Site E-commerce	This is the required method for credit card orders received through the Internet. • The unit requests a merchant ID from Treasury and required Web tool from OIT. • The unit establishes a Web site following the OIT procedures outlined for university Web sites processing credit cards.	Transactions are sent automatically via the payment processing services.

	• The Web site must reside on the OIT PCI-compliant infrastructure. • Authorization for use of any third party processor for payment transactions must be obtained from Treasury.	
Terminal and Printer (includes cash registers)	The unit purchases an electronic terminal and printer (through Treasury), which are connected to analog or data telephone lines. • The unit swipes the customer credit card to obtain authorization for the transaction. • A receipt is printed, which the customer signs. • Merchant receipts should be secured in a locked, limited access place. • Caution: If a terminal is IP-enabled, it must reside on OIT's PCI-compliant network and related infrastructure.	The day's receipts must be balanced and transmitted to the bank daily if there is one transaction or more. No transmittal is require if there are no transactions. No transmission equate to no sale. After 10 days the sale is void. Each additional day of non-transmittal of data results in a higher discount fee charged to the unit.
Cellular Card Reader	Unit must contact Treasury to order the necessary equipment for the following: • One-time events (rental services available) • Permanent solutions	Cellular functionality on

Managing Payment Cards

I. Third Party Service Providers

Units that outsource storage, processing, or transmission of cardholder data to third-party service providers must obtain from them annually, a Report on Compliance (ROC), which is evidence of a successfully completed PCI DSS assessment.

This documentation must be submitted to the OIT security office. In addition, units that are considering third-party outsourcing for credit card processing, or are renewing their current contracts, must consult with Purchasing and Treasury before signing a service contract.

II. Refunds

When an item or service is purchased using a credit and debit card and a refund is necessary, the refund must be credited only to the same account from which the purchase was made, unless the original credit or debit card account has been cancelled, in which case the refund may be issued to a different credit or debit

card. In addition, documentation of the original charge must be included with any refund transaction processed by the unit.

Caution: Under no circumstance is it permissible to issue a cash refund. To process a refund, follow the procedure appropriate to the mode of processing.

III. Handling a Customer Disputed Charge

The Bank is obligated to advise the Merchant, in writing, of a disputed charge. The Merchant is responsible to provide the Bank with written proof that the transaction was authorized by the Customer. Failure to respond or provide a copy of a receipt signed by the Customer or documentation of the shipping address will result in a Chargeback to the unit's account. All Bank requests for information concerning a dispute must be answered within two business days of receipt.

IV. Posting and Reconciling Transactions

It is important to record sales revenue accurately in the University financial records.

A unit is expected to reconcile internal records of sales activity to the designated general ledger account. If there is more than one category for either internal or external sales, the designated general ledger account becomes a clearing account, and the unit must distribute sales activity and "zero" these accounts via an accounting journal entry. Please contact Payments and Disbursements for additional information.

V. Canceling a Merchant ID

Should a unit decide that a Merchant ID (MID) is no longer needed, the unit must contact Treasury to cancel the MID. Likewise, the associated processing method must be properly disabled (see the "Decommissioning of Computer Systems and Electronic Media Devices" segment of this guide).

VI. Reporting a Breach

Units must develop a local incident response procedure approved by the OIT security office and train/inform all employees on procedures that must be adhered to when there is a suspected breach. Contact OIT security for additional details (provide link to contact info here.)

The Merchant Bank and the credit card agencies will consult to determine whether an independent forensic investigation will be initiated on the compromised entity.

Responsibilities and Approval Processes

I. E-Commerce: It is the responsibility of each campus unit to ensure all E-Commerce activities are managed in compliance with policy 6NEW (Payment Card Acceptance Policy).

II. Campus Units:

A. Determine if accepting Payment Cards will benefit the unit.

B. Consult with Treasury to determine the most efficient and secure processing method that meets unit business needs within the centrally developed processing structure.

C. Obtain written approval from Treasury before entering any contract or purchase of software and/or equipment for processing of Payment Card transactions regardless of the transaction technology used (e.g.-commerce, third party vendor, or payment terminals).

D. Do not negotiate contracts with credit card companies including on-line payment processors like PayPal.

E. Obtain a Merchant processing identity (Merchant ID) from Treasury by completing a Merchant application form.

F. Deposit all Payment Card revenue into designated University Bank accounts.

G. Maintain security standards and employ procedures as required by this policy, no matter what type of Payment Card processing is utilized.

H. Provide proper unit controls regarding who may process Payment Card transactions (e.g., terminal passwords may be established for return transactions).

I. Maintain a separation of duties between employees who process Payment Card transactions, those who reconcile daily batches, and those who post to the general ledger.

J. Charge sales tax where appropriate.

K. At month end, charge interchange and system related fees incurred for transaction activity to the unit department ID.

L. If Using Third-Party Outsourcing

1. Consult with Purchasing and Treasury before signing a service contract.

2. Annually submit to OIT a Report on Compliance (ROC), validating PCI DSS compliance of any third-party provider.

III. Treasury:

A. Coordinate with purchasing the negotiation of all contracts with credit card companies and all other providers of credit card processing systems, goods or services.

B. Consult with units regarding Merchant accounts, Merchant Discounts, web site security for payments, and all other aspects of this policy.

C. Authorize vendors used for payment transaction processing

D. Establish and maintain all depository accounts, Merchant accounts and Merchant account IDs.

E. Ensure appropriate accounting in conjunction with Payments & Disbursements.

F. Safeguard and track all credit card payment related activity.

G. Keep current with PCI DSS regulations and make changes to processes, as appropriate.

H. Arrange for the provision of rental credit card processing units as needed by the units.

IV. Purchasing:

A. Consult with Treasury and units regarding service contracts for third-party outsourcing of PCI-compliant credit card processing systems.

B. When evaluating contracts, verify that the contract states that it will become null and void if the vendor does not maintain PCI DSS compliance.

V. Office of Information Technology:

A. Coordinate unit technical implementation and changes for credit card processing

B. Keep current with PCI DSS regulations and make changes to tools, systems and processes, as appropriate.

C. Consult with units on technical PCI DSS issues.

D. Assist units when there are data breaches.

E. Conduct mandatory annual training sessions in accord with University policy #6NEW (Payment Card Acceptance).

F. Coordinate and account for annual PCI DSS requirements:

1. Collect, review, and remit to the PCI Security Standards Council annual Self-Assessment Questionnaires from the units processing credit cards

2. Coordinate and review quarterly scans of cardholder data

3. Confirm that units using third-party providers have submitted proper documentation

VI. Individuals

Report any breaches to the OIT Security Office and Treasury, according to the "Reporting Breaches" section of the Payment Card Acceptance Information and Procedure Guide.

***

Payment Card Security and Ethics Certification Form

The following page is a statement of understanding and intent to comply with the University Payment Card Acceptance Policy.

Anyone who has access to credit or debit card information must sign the form and submit it to his or her Department Supervisor on an annual basis.

Boise State University

Payment Card Security and Ethics Agreement

Applicable to: Any individual who accepts, captures, stores, transmits and/or processes credit or Debit card information

Effective Date: May 2015
Many University departments accept credit/debit card information, such as credit/debit card numbers, expiration dates and card verification codes, from donors, purchasers of University publications and services, etc.

I recognize this information is sensitive and valuable and that the University is contractually obligated to protect this information against its unauthorized use or disclosure in the manner defined by the Payment Card Industry's Data Security Standard, and should such information be disclosed to an unauthorized individual, the University could be subject to fines, increased credit and debit card transaction fees and/or the suspension of our credit and debit card privileges.

As an individual whose role includes the acceptance, capture, storage, transmission and/or processing of credit and/or debit card information, I agree with the following statements:

A. I have read the requirements stated in the University's Payment Card Acceptance Policy.

B. I understand that I may only accept credit and debit card payments using methods approved by the University IT Security Officer and the Treasurer's Office.

C. I understand that, as an individual who has access to credit and debit card information, I am responsible for protecting the information in the manner specified within the Policy. Further, I understand that I am also responsible for effectively protecting the credentials (IDs and passwords) and the computers that I may use to process credit or debit card transactions.

D. I understand that I must destroy credit and debit card information as soon as it is no longer necessary using methods prescribed by the Payment Card Acceptance Information and Procedure Guide, Companion to University policy 6xxx).

E. I understand that in cases where I suspect that a breach of credit or debit card information has occurred, I must immediately report the breach to the University IT Security Officer.

F. If I manage an area that handles credit card information, I understand that I must have appropriate checks and balances in the handling of credit and debit card information, and that I am responsible for having documented procedures in place for complying with Policy.

G. I commit to comply with the Policy and its documented procedure, and understand that failure to comply with the above requirements may subject me to a loss of credit and debit card handling privileges and other disciplinary measures. For employees, non-compliance could result in termination of employment.

Signature: _____ Date: _____

Print Name: _____