Boston College Policy

ACCEPTING PAYMENT CARDS FOR CONDUCTING UNIVERSITY BUSINESS:

PURPOSE OF POLICY:

The purpose of this policy is to establish procedures for accepting payment cards at Boston College that will minimize risk and provide the greatest value, security, and service to each university unit within the rules, regulations and guidelines established by the Payment Card Industry (PCI).

WHO IS AFFECTED BY THIS POLICY:

All university units that are involved in the acceptance of payment cards on behalf of Boston College are affected by this policy. This includes employees, contractors, consultants, temporary employees and other workers in the university units. This policy also applies to external applications linked to a Boston College website which accept payment cards and external vendors who collect, process, or store payment card data on behalf of Boston College.

WHO SHOULD READ THIS POLICY:

Any university unit that conducts business on behalf of Boston College through payment card transactions and any university unit responsible for developing and/or maintaining the infrastructure surrounding accepting payment cards (i.e. website, software programs, etc…)

CONTACTS:

Cash Services	617-552-0789
Information Technology Services	617-552-6060
Procurement Services	617-552-3055
Internal Audit	617-552-3258

WEBSITE LOCATION OF POLICY:

http://www.bc.edu/offices/controller/

CONTENTS OF POLICY:

DEFINITIONS:

These definitions apply to these terms as they are used in the following policy:

Cardholder:	Customer to whom a card is issued or individual authorized to use the card.
Cardholder Data:	Any personally identifiable data associated with the cardholder. This could be an account number, expiration date, Card Validation Code CVC 2 (Mastercard), Card Verification Value CVV2 (VISA), or Card Idenitifcation Number – CID (American Express).
Cash Services:	Office within the Controllers Office that approves all third party service providers and coordinates the policies, practices, and procedures for accepting payment cards at Boston College.
CASHNet:	Software application used by Boston College for recording transactions related to cash, checks, or payment cards. **Commerce Center:** providing secure, system-wide campus commerce solutions allowing departments to accept and authorize and deposit credit cards and checks using their PC. **CASHNet eMarket:** includes Storefront, Checkout, and Transaction Gateway solutions that can be used independently or together, allowing various campus-wide departments to seamlessly accept and authorize payments. Types of payments are determined by the individual department and can include alumni donations, theater tickets, apparel, or event and conference registration fees. At checkout, the user will click "pay here" and the transaction will be transmitted to the credit card processor.
Chargeback:	The deduction of a disputed sale previously credited to a university unit's account when the unit fails to prove that the customer authorized the credit card transaction.
Payment Cards:	Credit cards or debit cards issued by a financial institution.
PABP:	Payment Application Best Practice (PABP) is software installed on a computer and determined by the credit card industry (PCI) to follow the industry's best practices for securing credit card information.
Payment Card Industry:	Payment Card Industry (PCI) is a council formed by the credit card industry (VISA, Mastercard, Discover and American Express to establish Data Security Standards (DSS) for the industry. https://www.pcisecuritystandards.org/

Point-of-sale Terminal:	A point-of-sale (POS) terminal is an electronic terminal and printer (connected to a phone line) where the university unit swipes a credit card to obtain authorization for the transaction. A receipt is printed which the customer signs.
Nelnet QuickPay:	Ecommerce application that accepts and processes payment cards.
University Unit:	A department, service center, student organization, or other university entity that accepts payment cards to conduct business.

OVERVIEW OF POLICY:

Payment cards may be accepted by university units for various purposes, including the sale of goods or services, and donation of gifts. Cash Services may immediately remove any university unit's ability to accept payment cards if that unit's actions violate any part of this Policy or puts Boston College at risk. Please contact Cash Services if you have any questions regarding permitted transaction types.

Acceptable Payment Cards:

Boston College currently accepts VISA, MasterCard, Diners Club, and American Express cards. Boston College has negotiated contracts for processing payment card transactions. Individual university units must not attempt to negotiate individual contracts with these or other payment card companies or processors.

Prohibited Payment Card Activities:

Boston College prohibits certain credit card activities that include, but are not limited to:

- accepting payment cards for tuition and fees unless special approval is granted by the Student Services
- accepting payment cards for cash advances
- discounting a good or service based on the method of payment
- adding a surcharge or additional fee to payment card transactions**. (**charging the cost of processing a payment card transaction back to the cardholder violates some card brands' rules, and the practice is illegal in Massachusetts.)
- using a paper imprinting system unless special approval is granted by Cash Services.

Payment Card Fees:

Each payment card transaction will have an associated fee charged by the credit card company. At the end of each monthly billing cycle, payment card fees will be allocated to the PeopleSoft general ledger account identified by the university unit.

Refunds:

When a good or service is purchased using a payment card, and a refund is necessary, the refund must be credited back to the account that was originally charged. Boston College prohibits refunds in excess of the original sale amount and cash refunds.

Chargebacks:

Occasionally a customer will dispute a payment card transaction, ultimately leading to a chargeback. In the case of a chargeback, the university unit initiating the transaction is responsible for providing additional information to the Cash Services Office at Boston College. If not resolved, the transaction will be charged back against the university unit's PeopleSoft general ledger account.

Maintaining Security:

- Every university unit accepting payment cards on behalf of Boston College is subject to the Payment Card Industry Data Security Standards (PCI DSS). https://www.pcisecuritystandards.org/
- Boston College limits payment card data transmission via fax, e-mail, unsealed envelopes through campus mail, or wireless networks, as these are not secure.
- Boston College requires that all external service providers be PCI compliant.
- Access to cardholder data is restricted to those with a business "need to know."
- Each person with access to cardholder data electronically has a unique password.
- For electronic media, cardholder data should not be stored in its entirety on servers, local hard drives, or external (removable) media including floppy discs, CDs, and thumb drives (also called flash drives) unless encrypted and otherwise in full compliance with PCI.
- For paper media (e.g. paper receipts, forms, and faxes), cardholder data should not be stored, unless approved for appropriate business purposes and access is limited to individuals with a business need to know. Cardholder data should be "blacked" out on paper media, and disposed of properly (e.g. shredded) when no longer needed for business purposes.

PROCEDURES:

Obtaining Approval to Process Payment Cards:

1 University unit completes the Payment Card Processing Request & Agreement Form.

2 Cash Services works with the university unit to determine whether an existing approved system (e.g. CASHNet, Nelnet Quick Pay) will meet their requirements and conducts a site survey to identify requirements for point-of-sale (POS) terminals and other hardware and software.

3 The university unit administrator executes the Terminal Hardware Agreement, if required.

Methods of Processing Payment Card Transactions:

- **In-person, phone, or mail:** Using a stand alone Point-of-Sale (POS) Terminal or CASHNet Commerce Center to process transactions, cardholder information is entered by department staff.
- **Secure website:** The university unit works with Cash Services and ITS (Information Technology Services) to use the university units' existing website to establish links to the secure gateway for payment. In this instance CASHNet eMarket or Nelnet Quick Pay will be used to process transactions.

RESPONSIBILITIES:

University Units need to ensure that:

- Only authorized personnel have access to payment card applications and data.
- Payment card account numbers are properly secured and safeguarded (see "Maintaining Security" section above).
- PeopleSoft accounts are properly reconciled to detailed support and any discrepancies are brought to the attention of Cash Services immediately. To maintain proper segregation of duties and minimize the risk of fraud the individual reconciling the PeopleSoft Account is not the same individual that initiates, authorizes and processes the transactions.
- Cash Services is notified immediately of any changes in a unit's card processing environment; including using the account for a new purpose, adding a new card acceptance technology or channel, or adding or customizing a payment application.
- Cash Services is notified if the university unit contemplates entering into an agreement with any external application or vendor that collects credit card data from the unit's customers.
- Access to payment applications is restricted to appropriate individuals as outlined in the Boston College Payment Card Processing Request & Agreement Form.

Cash Services needs to:

- Provide training to ensure that university unit staff is trained in accepting and processing payment cards in compliance with the Boston College Policy: Accepting Payment Cards for Conducting University Business and PCI standards.
- Work with university unit(s) to create and test payment card accounts before implementation.
- Work with external vendors and coordinate the policies, practices, and procedures for accepting payment cards at Boston College.
- Verify annually that payment applications are PCI compliant and, if applicable, on the Payment Application Best Practice (PABP) list
- Liaison between FMS/Information Technology Services and the university unit in the initial implementation phase.

Information Technology Services:

- In conjunction with the university unit's data security officer, identify compliant application software or service providers with the required functionality to meet university business needs.
- In conjunction with the university unit's data security officer, complete the PCI Self Assessment yearly and coordinate with external scan vendor(s) quarterly to ensure PCI compliance.
- Ensure that all router, switches, wireless access points, and firewall configurations are properly secured.

Procurement Services:

- Reviews of contracts with external vendors to ensure that language exists to protect the University.
- Ensure that the Privacy and Security Addendum is signed by all external vendors that store, transmit, or use private data.
- Is authorized to communicate with external vendors to process payment card transactions.

Internal Audit:

- Annual validation that university units are complying with the Payment Card Industry (PCI) Data Security Standards (DSS).
- In the course of internal audits,
    - Identify unapproved payment applications and external vendors that collect payment card data on behalf of the university unit's customers and notify Cash Services.
    - Review university unit procedures to ensure adherence to the Boston College Policy: Accepting Payment Cards for Conducting University Business.

ADDITIONAL INFORMATION:

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

https://www.pcisecuritystandards.org/

Visa website:

http://usa.visa.com/?country=us&ep=v_gg_new

Mastercard website:

http://www.mastercard.com/us/gateway.html

American Express website:

https://home.americanexpress.com/home/mt_personal.shtml?