PAYMENT TRANSACTIONS POLICY

Effective: March 3, 2021

Revision History: Initial release

Executive Summary: This policy establishes the requirements for the acceptance and processing of credit card payments at Barnard College and for the protection of Cardholder Data in accordance with the Payment Card Industry Data Security Standards (PCI -DSS). This policy aims to ensure that College Merchants are aware of their responsibilities:

- Store and maintain Cardholder Data appropriately
- Restrict access to Cardholder Data
- Use approved payment devices/solutions, and
- Maintain awareness of information security practices and incident response procedures

Reason for the Policy: This policy sets the standards for protecting Cardholder Data supplied to the College or any Third-Party Service Provider acting on behalf of the College. Failure to follow this policy would prevent the College from being able to accept and process credit card transactions and could significantly increase our compliance burden. In addition, failure to follow this policy would expose the College and members of the Barnard community to financial fraud, fines and penalties, and reputational harm.

Who is Responsible for This Policy:

Responsible Administrator:	Chief Financial Officer & VP for Finance
Responsible Offices:	Finance BCIT, Information Security

Who is Governed by This Policy: All College employees, students, volunteers, and third parties who handle Cardholder Data on behalf of the College or can impact the security of the College's Cardholder Data Environment are governed by this policy.

Definitions:

Cardholder Data - At a minimum, consists of the full Primary Account Number but may also include the full Primary Account Number with cardholder name, expiration date, or service code.

Cardholder Data Environment (CDE)- The people, processes and technology that capture, store, process or transmit Cardholder Data, including any system components that may affect the security of such data.

Merchant – Any department that accepts credit cards, payment wallets, or electronic currency as payment for goods and/or services on behalf of the College.

PCI DSS - Payment Card Industry Data Security Standards – provides a baseline of technical and operational requirements designed to protect Cardholder Data and applies to all entities that store, process or transmit Cardholder Data and/or are involved in credit card processing.

P2PE – Point to Point Encryption – cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. At no point in the process is the Cardholder Data transmitted or stored in clear text or human readable format.

Primary Account Number (PAN) – and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account, and consists of 16 to 19 digits.

Sensitive Authentication Data – Security related information used to authenticate cardholders and/or authorize credit card transactions, includes full track data, equivalent data on the chip, three- or four-digit code (e.g., CVV), or Personal identification number (PIN) entered by cardholder during a card present transaction, and/or encrypted PIN block present within the transaction message.

Third-Party Service Provider – business entity that is directly involved in the processing, storage, or transmission of Cardholder Data or that provides services that control or could impact the security of the Cardholder Data Environment.

Policy Statement: Any Barnard College department or function that accepts credit card or other forms of payment transactions for events, subscriptions, fees, donations, and merchandise on behalf of the College or College sanctioned activity must ensure that all processes, operational procedures, and related technologies used for accepting credit card and other payment transactions comply with PCI DSS and relevant College policies.

The following standards are defined to assist the College with adhering to this Policy.

Merchant Designation and Responsibilities

- Merchant IDs (MIDs) can only be obtained through the Chief Finance Officer and must be approved by the requesting department's Senior Staff representative.
- Merchants must validate and get approval from BCIT Information Security for their Cardholder Data Environment (CDE) prior to processing any transactions and prior to implementing any changes to their existing CDE.
- Merchants must be able to describe their CDE. The CDE description must include all data flows, Point of Sale devices, network devices, servers, computing devices, applications and any other component or device located within or connected to their CDE. The description and any associated documentation must be made available to BCIT Information Security for review upon request.
- Merchants are expected to maintain a signed *Duty of Confidentiality Acknowledgement* for all individuals assigned roles and responsibilities associated with credit card processing for their department.
- Merchants must ensure that all Third-Party Service Providers that may affect the security of the Merchant's Cardholder Data or could have an impact on the Merchant's CDE must be approved through the College's Procurement Service prior to requesting a new MID or being associated with an existing MID.
- Merchants must maintain copies of Third-Party Service Provider documentation indicating which PCI DSS requirements will be met by the Third-Party Service Providers and which will be the responsibility of the Merchant.
- Merchants must obtain valid (i.e., unexpired) proof of Third-Party Service Provider's PCI DSS compliance on an annual basis.
- Merchants must review transactions prior to settlement, ensure all open batches are settled daily, and reconcile all account activity (including fees) at least monthly. Reconciliation procedures must be approved by the College's Controller.
- Merchants must take immediate action to respond to a suspected or confirmed security compromise of the CDE or any Cardholder Data by notifying individuals identified in below section "Responding to a Suspected Cardholder Data Breach."

Protect Cardholder Data
Barnard strictly prohibits Cardholder Data from being captured, stored, processed, or transmitted on College servers or networks with the following exceptions:

- Transmission of encrypted Cardholder Data is permitted through a PCI validated Point-to-Point Encryption (P2PE) Solution (see "Approved Methods of Accepting Credit Cards").
- Storage of paper forms and digital images of Cardholder Data is permitted only when such data is rendered unreadable (see "Data Retention and Storage").

Approved Methods of Accepting Credit Cards
The following methods are approved for use to accept credit card transactions on behalf of the College:

Point-of-Sale (POS) (face-to-face) / Card-Present:

- P2PE Device listed on the PCI Council's List of PCI P2PE Validated Solutions
- Stand-alone terminal with dial-up connection to a dedicated phone line (*IP/Internet connections are prohibited for stand-alone terminals*)
- Handheld terminal enabled with Cellular connection (*mobile phone card readers are prohibited*)

Mail order/telephone order (MOTO) / Card-not-Present:

- College approved software and hardware only

E-Commerce / Card-not-Present:

- Outsource all e-commerce functions and technology support to a College approved PCI compliant vendor

Additional information on currently approved methods, solutions, and devices is provided on the Barnard Payment Transaction resources page available under myFinance on the myBarnard portal.

Device Security
Barnard owned equipment that has direct physical interaction with Cardholder Data must be approved by BCIT Information Security prior to use, maintained through a documented chain of custody, and periodically inspected to ensure that it continues to protect Cardholder Data and operates as expected.

- BCIT, Director Information Security or her designee is the named custodian for all equipment that has direct physical interaction with Cardholder Data. The custodian maintains records regarding the equipment including inventory, status, location, tamper inspections, and attestations.
- BCIT, Director Information Security or her designee will prepare attestations on PCI DSS compliance at least annually and provide them to the Chief Finance Officer for review and signature.
- Merchants must verify the identity of any persons claiming to be repair or maintenance personnel prior to granting access to troubleshoot or modify the device.
- Merchants must not install, replace or return devices without verification of the device chain of custody in coordination with BCIT Information Security.
- Merchants must maintain awareness of device tampering and must perform inspections using the "*Device Inspection Checklist*" periodically, particularly when loaned devices are returned or after maintenance is performed. The "*Device Inspection Checklist*" will be provided by or confirmed by the BCIT, Director Information Security or her designee to ensure the checklist is specific to the device or devices known to be in use by that Merchant.
- Merchants must take immediate action to respond to any indications of device tampering by notifying individuals identified in below section "Responding to a Suspected Cardholder Data Breach."

Data Retention and Storage
Storage of Cardholder Data is only permitted in the form of paper documents and/or digital images of such paper documents and must adhere to the following:

- Documentation containing the full PAN may only be securely stored in paper form and only until authorization, at which point the full PAN must be rendered unreadable with no more than the first six and/or last four digits visible, i.e., the use of a black or opaque marker to obscure the necessary digits.

- Storage of Sensitive Authentication Data is never permitted and must be rendered completely unreadable immediately.
- The PAN and Sensitive Authentication Data must be rendered unreadable before the document is imaged and scanned for any digital storage.
- All paper records must be stored in a safe, secure and monitored area with access limited to select personnel on a "need to know" basis only. A locked room is not enough if the storage space is in a shared environment that is accessible to those without a "need to know," such as janitorial staff. Storage space or cabinets need to be locked in those situations.
- All digital records must be saved to a secure file location on a drive with limited and monitored access to select personnel on a "need to know" basis only.
- Retention periods must be limited to that which is required for business, legal, and/or regulatory purposes
- Merchants must have a process in place to review the need for any stored paper records on a quarterly basis.

After the designated retention period:

- Hard-copy documentation must be crosscut shredded, incinerated, or pulped either by the Merchant or through a contract with an approved Secure Destruction vendor, such that there is reasonable assurance the hard-copy documents cannot be reconstructed.
- Digital images of documentation must be rendered unrecoverable, e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media.

Awareness and Training

Required training on the appropriate procedures to protect Cardholder Data, identify device tampering and report potential Cardholder Data compromise must be completed by all individuals with access to the Merchant CDE, first upon hire or upon assuming a new role that requires such access, then on an annual basis thereafter, for as long as the individual has access to any Barnard Merchant CDE.

Responding to a Suspected Cardholder Data Breach

Anyone with knowledge or suspicion that Cardholder Data has been compromised in any way must immediately report the incident to each of the following:

- Immediate supervisor
- BCIT: help@barnard.edu or the Director, Information Security (bcit-infosec@barnard.edu)

BCIT will coordinate with the Chief Financial Officer, Office of General Counsel, and other appropriate departments to determine next steps.

BCIT will also work with the Merchant to take immediate steps to preserve all business records, logs and electronic evidence.

Enforcement and Compliance

Merchants at the College are subject to periodic audit to support the College's PCI DSS compliance obligations and to ensure we are maintaining our standards to protect Cardholder Data. Violations of PCI DSS or College policies can result in the termination of the Merchant's ability to accept credit cards as a method of payment. Individuals may also be subject to disciplinary action.

Related Policies and Documents:

Payment Card Industry Data Security Standard (PCI DSS):
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

Barnard College Purchasing Procedures: https://barnard.edu/purchasing/procedures

Barnard's Payment Transaction Frequently Asked Questions and other supporting documentation is available in myFinance section of the myBarnard portal

Website for This Policy: my.barnard.edu/BC%20Policies/Payment%20Transactions%20Policy.pdf