Policy on the acceptance and handling of credit cards

Brandeis University is committed to providing a secure credit and debit card processing environment for our customers to protect against loss and fraud. To protect customers and limit University liability, we must comply with Payment Card Industry (PCI) requirements for securely processing, transmitting, and disposing of cardholder data. This policy will be effective immediately upon final approval. Final approval on:

Contents:

A. Definitions

Owner: The senior employee with direct responsibility for all credit card payment processing activities for their department or unit.

Contact: The documented employee on file responsible for maintenance and coordination of payment card systems for their department or unit.

Operator: Any employee tasked with processing card payments for their department or unit.

Cardholder data: Any payment card information that is processed on behalf of Brandeis University. This includes card numbers, expiration dates, security codes (located on the back of credit cards) and card holder personal data.

PCI-DSS: Payment Card Industry – Data Security Standards.

PA-DSS: Payment Application – Data Security Standards.

SAQ: Self-Assessment Questionnaire.

Merchant: Any University unit that accepts debit or credit cards as part of its business process.

Vendor: Any person or company contracted by the University to facilitate payment card transactions.

Critical Technology: Any technology device used within, or to connect to or from, the payment card processing environment network or equipment.

University Information Security Office: the Security Office within LTS

B. Policy.

All Brandeis University owners, contacts, and operators of any point-of-sale systems, credit payment terminals, or credit processing systems must maintain compliance with current PCI-DSS.

B-1. Pre-approval:

(1) Only merchants and vendors pre-approved by Office of Treasury Services are authorized to handle University credit card processing. Third-party vendors or service providers contracted by a merchant must supply a contract addendum or other certification assuring their compliance with the current PCI-DSS and/or PA-DSS as appropriate. If applicable, a list of service providers must be maintained by the department or unit contact, and the compliance status of each vendor must be verified at least annually. No business process or system that electronically stores, processes or transmits cardholder data will be approved for operation within the Brandeis environment.

(2) No storage of cardholder data is permitted (in any format, digital or paper) is permitted at Brandeis.

B-2. SAQ Completion Responsibility:

Prior to operation of any payment card processing system, and on an annual basis at a time communicated from the Office of Treasury Services with at least 30 days of notice, each department or unit must complete a PCI-DSS Self-Assessment Questionnaire (SAQ) for each operated merchant, along with a corresponding Attestation of PCI Compliance. These must be jointly reviewed and approved by the University Information Security Office and the Office of Treasury Services.

B-3. Personnel:

(1) At the onset of employment, and at least annually thereafter, all owners, contacts and operators directly involved with acceptance or processing of payment card data for the University must complete a comprehensive PCI-DSS compliance and security awareness training as required by the Office of Treasury Services. Such training must be in accordance with the list of recommended trainings as approved by the Security Office. Annual training must include a review of this policy and any standards set by management to ensure PCI compliance. Any department or unit specific processes or procedures must also be reviewed annually with each operator and internally documented by the department or unit for the SAQ.

B-4. Documentation:

Any department or unit operating payment card systems must maintain documentation of all procedures for handling payment card data and systems consistent with PCI-DSS. Documentation required of PCI-DSS and this policy must be readily available during business hours at request of the Office of Treasury Services or the Brandeis University Information Security Office.

B-5. Inventory: Any department or unit operating payment card systems must maintain a list of current devices used to process credit cards or used in the cardholder environment and be aware of attempted tampering or replacement of devices. Each device must be appropriately labeled. This list must be supplied to the Office of Treasury Services annually. The inventory list must include:

- Make and model of devices
- Location of each device
- Device serial number or asset tag

B-6. Usage policies for critical technologies:

(1) All critical technology used within the payment processing environment must be explicitly approved by the Office of Treasury Services and Security Office and inventoried prior to operation.

(2) Only employees trained in Merchant processes and this policy are permitted to use critical technology, and only if required by their job function.

(3) All employees using critical technology must be authenticated with a user ID and password (or other authentication item or token).

(4) Critical technology must only be used for designated business purposes and not for general administrative use which might increase risk to the payment processing environment (e.g., no email, web surfing, instant messaging, etc.).

(5) Critical technology may only be used on networks approved and designated for payment card processing. Please contact LTS Security Office for review and approval.

(6) Remote access to critical technologies must:

a. Be limited to only uniquely identified employees or vendors with a business need;

b. Be configured to automatically disconnect when inactive;

c. Restrict vendor or support partner access accounts to active monitoring, with immediate deactivation after use.

(7) Copying, moving or storing cardholder data on local hard drives or removable electronic media is prohibited.

B-7. Reporting Incidents: In the event of a suspected incident, event, or tampering potentially involving the exposure of cardholder data, immediate notification of the incident must be sent to the following groups:

- LTS Security Office (security@brandeis.edu)
- Office of Treasury Services (treasury@brandeis.edu)
- The owner for the Merchant ID

After the incident has been reported, it shall be investigated and escalated in accordance with the Technology Security Incident Response Plan and current PCI requirements.

B-8. Standards: Technical standards are required by PCI-DSS and published regularly on the PCI Security Standards website. Complying with the published standards are required in order to complete annual SAQ successfully and remain compliant. https://www.pcisecuritystandards.org/

B-9. Consequences: Failure to remain in compliance with the terms of this policy will result in the loss of the ability to process credit cards and the required payment of assessed fines/fees/penalties until PCI compliance has been regained to the satisfaction of the Office of Treasury Services and the LTS Security Office.

C. Scope. This policy applies to all entities processing credit cards directly or on behalf of Brandeis University

D. Process, Procedure, and Guideline. Additional guidelines, processes, and procedures may be distributed or published by the Office of Treasury Services and LTS in support of this policy and current PCI standards. Please see their websites for current information.

E. Exceptions. Due to the need to remain in compliance with PCI DSS standards, exceptions will not be granted to this policy.

F. Contact Information. The Office of Treasury Services and the Security Office can assist with questions regarding this policy and PCI compliance.

Office of Treasury Services info: Phone: 781-736-4541 or treasury@brandeis.edu
http://www.brandeis.edu/business-finance/contacts/

Security contact info: Phone: 781-736-4560 or security@brandeis.edu