Office of Finance and Treasury
How to Accept & Process Credit and Debit Card Transactions

1) Only authorized and properly trained individuals can process credit or debit card transactions and access systems or reports containing credit or debit card information. A list of authorized individuals and their job title must be provided to Finance Technology, and updated annually.

2) Individuals who handle or process credit and debit card information at Princeton University:
   a) Must be authorized by their appropriate academic or administrative department manager, dean or director.
   b) Must be trained in the proper handling of credit or debit card information. This requirement shall be met by completion of the University’s PCI Compliance Training Program available through the Princeton University Employee Learn Center.
   c) Must be familiar with, and adhere to, the University’s Information Security and Acceptable Use Policy.
   d) Must protect cardholder information in accordance with PCI-DSS.
   e) Must pass a criminal background check.
      i) Job descriptions for any position with responsibilities that include handling or processing cardholder data, or maintaining systems that contain cardholder data, must specify that passing a background and credit check is a requirement for the position.
      ii) In cases where a background check returns outstanding issues, the appropriate department manager, dean or director must review those issues with Human Resources and the Office of the General Counsel to determine whether or not the individual should be permitted to handle cardholder data.
      iii) Exceptions to this requirement may be granted by Cash and Investment Services only if an individual processes over-the-counter or over-the-phone credit or debit card transactions, and does not have access to lists, reports and/or storage areas with cardholder data.

3) University Systems and Applications in the Cardholder Data Environment (CDE)
   a) Must limit access to only those individuals whose jobs require such access. User privileges must be based on job function, and access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities.
   b) Applications processing credit card transactions are configured so that only a System Administrator can add users to the system.
   c) Only individuals authorized by the unit manager are added to the system by the System Administrator.
   d) Each authorized user has a unique account and password, and does not share their account and password with anyone.
   e) Use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.
   f) Access to and querying of the cardholder data is restricted to a system administrator.
   g) Access to systems with cardholder data is revoked immediately if a user is terminated.
   h) Cardholder data may not be saved, copied, or moved onto local hard drives or removable electronic media.

4) Methods Approved for Acceptance of Credit or Debit Cards
   a) Credit or debit card payments may be accepted using only the following approved methods:
      i) Card Present
         (1) Credit card dipped, tapped or swiped through a card reader that is part of a PCI validated P2PE (Point to Point Encryption) solution, approved by Finance Technology.
   b) Card Not Present
      i) Cardholder data communicated verbally over the phone
      ii) Cardholder data received in writing on a secure analog fax or by US Mail
      iii) Cardholder data entered into a third party PCI-DSS-compliant payment application approved by Finance Technology.
iv) Cardholder data entered into a Princeton University website with a secure PCI compliant gateway integrated via an iframe approved by Finance Technology.

c) Transmission of cardholder data via end user messaging, including E-mail, instant message, chat or other clear-text method is strictly prohibited.

5) Methods Approved for Processing of Credit or Debit Card Transactions
   a) Computers / Terminals
      i) Only centrally managed University owned computers, approved terminals and Devices, and servers can be used to process credit or debit card transactions. Any exceptions must be approved by Information Security Office.
      ii) Computer/terminals used to process credit or debit card transactions must be labeled as a machine used to process credit cards, with owner’s name and contact information.
      iii) A complete list of computers/terminals used to process credit or debit card transactions must be provided to Cash and Investment Services by each Merchant Location annually. The list must include the make, model, serial number, and location of each machine.

   b) When using a terminal to process credit or debit card receipts.
      i) Payment cards must be dipped, tapped, swiped or read by NFC means as allowed by its P2PE Instruction Manual (PIM)
      ii) Terminals must be set to automatically settle daily.
      iii) Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both customer and merchant receipts, and on any reports that may be produced by the device.

   c) The following wireless and mobile devices are currently not approved for the acceptance and processing of credit or debit card transactions.
      i) Card readers (e.g. Square and other devices) that connect to mobile phones, tablets, or other wireless devices.
      ii) Wireless keyboards

6) E-Commerce
   a) University websites that accept online payment by credit or debit card and redirect users to a secure payment gateway must be reviewed and approved by Finance Technology and OIT. The web server must be located in a secure environment approved by OIT. It must be an OIT managed server or at a Service Provider that is approved by Finance Technology. Secure gateways are only permitted, if they have been approved by Finance Technology.

   b) Appropriate software development practices need to be followed for the creation and maintenance of any website or applications that store, process, or transmit cardholder data or that can impact the security of the Cardholder Data Environment. Prior to development, the department should contact Finance Technology for a list of current practices and/or to discuss options

   c) For any website or application that can store, process, or transmit cardholder data or that can impact the security of the Cardholder Data Environment, all applicable vendor-supplied security patches should be applied within an appropriate time frame, preferably within 3 months. Any critical security patches should be applied within 1 month.

7) Third party applications software that accepts payment by credit card must be approved by Finance Technology. Prior to implementation the Department must conduct required due diligence on the software application in conjunction with Finance Technology, to ensure that the application is properly configured, and to determine how cardholder data is captured, transmitted and stored by the application.
   a) Third party software applications should be configured to utilize a secure gateway and must be reviewed and approved by Finance Technology.
   b) Service Providers must contractually assume responsibility for the security of cardholder data they handle on behalf of the University, and Service Provider contracts must be reviewed and approved by Finance Technology for PCI language and confidentiality provisions. All Service Provider contracts, and contract renewals executed
by a department must be submitted to Finance Technology.

b) If a Service Provider updates its terms and conditions, save a copy for your records. During the annual
departmental attestation, send a copy of the updated terms and conditions, to Finance Technology.

d) Each year the Department must verify with Finance Technology that any third party software applications used
by the Department to process cardholder data are PA-DSS compliant, and any third party Service Provider used
by the Department to process cardholder data have been certified by VISA/MC as a compliant service provider.

e) Except on computers/terminals/registers used only for cashiering at a point of sale, the Application must be
configured to meet all PCI requirements for User IDs and passwords which are not satisfied by the University’s
general network:

i) Disable inactive user accounts within 90 days.

ii) Require users to change their passwords at least every 90 days and submit a new password that is different
from any of the last four passwords he or she has used

iii) Lock out user ID’s after no more than six failed attempts, with lockout duration set to a minimum of 30
minutes or until an administrator enables the User ID

iv) Require strong passwords with minimum length of at least 7 characters that contain both numeric and
alphabetic characters

v) Verify user identity before permitting modification to any authentication credential, such as a password
reset or provisioning of new token

vi) Require users to re-authenticate or re-activate the session after being idle for more than 15 minutes.

vii) Login via remote access to applications handling cardholder data requires use of multi-factor
authentication.

8) Segregation of Duties

a) In order to minimize manual errors and ensure compliance with PCI requirements, the segregation of credit and
debit card handling duties is required.

b) The processing of credit or debit card transactions, refunds, and monthly reconciliation must be performed by
two or more individuals.

c) In departments where the segregation of duties is not feasible, alternative and compensating controls may be
implemented to achieve the desired objectives. Please contact Cash and Investment Services on how to
establish appropriate controls for your area.

d) The department manager is responsible for ensuring that Cash and Investment Services is aware of any changes
in personnel or job descriptions that impact the segregation of duties.

9) Reconciliation of Processed Credit or Debit Card Receipts

a) Credit or debit card settlements from terminal receipts or web-based reports should be reconciled against the
ledger detail report and merchant account statements. Reconciliations must be maintained by the department
and are subject to review by Cash and Investment Services.

b) Reconciliations must be performed at least monthly and must be signed and dated. Daily reconciliations are
strongly recommended.