Office of Finance and Treasury

How to Accept & Process Credit and Debit Card Transactions

<table>
<thead>
<tr>
<th>Related Policy Title</th>
<th>Credit Card Processing Policy For University Merchant Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Executive</td>
<td>Carolyn Ainslie, vice president for finance and treasurer</td>
</tr>
<tr>
<td>Responsible Office</td>
<td>Office of Finance and Treasury</td>
</tr>
<tr>
<td>Contact</td>
<td>Hanna Bigelow, cash manager, <a href="mailto:hbigelow@princeton.edu">hbigelow@princeton.edu</a> or 258-5056</td>
</tr>
<tr>
<td>Effective Date</td>
<td>February 1, 2016</td>
</tr>
</tbody>
</table>

I. PURPOSE OF PROCEDURE

Each department that accepts, captures, stores, transmits, or processes credit or debit card payments must follow basic minimum procedures related to the Credit Card Processing Policy For University Merchant Locations. This procedure defines how credit and debit payments should be accepted and processed.

II. WHO IS AFFECTED BY THIS PROCEDURE

Any individual who accepts, captures, stores, transmits, or processes credit or debit card transactions on behalf of the University.

Any individual with access to systems or reports containing credit or debit card information. Common examples include technical support staff responsible for maintaining computers containing credit or debit card information, and individuals tasked with shredding cardholder data.

III. CONTENTS LINKS

POLICY STATEMENT
WHO IS AFFECTED BY THIS POLICY
CONTENTS LINKS
DEFINITIONS
POLICY
PROCEDURES
FORMS
CONTACT ROLES AND RESPONSIBILITIES
UPDATE LOG
IV. Definitions

**Approved Terminals and Devices**
Terminals and devices used to process credit or debit cards at the University must be reviewed and approved by the Office of Information Security and Cash Management, and must be sourced from designated vendors. A list of Approved Terminals and Devices can be found on the Cash Management website.

**Certification of PCI Compliance**
Each year PCI Compliant Service Providers must be audited by a QSA who confirms and certifies their compliance with the most current PCI standards. Service Providers that receive this certification register with Visa/Mastercard, and appear on the Visa/Mastercard list of PCI Compliant Service Providers. Certifications of PCI Compliance are obtained from the Service Provider or from Visa/Mastercard’s website.

**Credit card**
A banking instrument used in credit transactions which is issued to cardholders by a financial institution, and is commonly accepted as a form of payment. A credit card allows its holder to buy goods and services based on the holder’s promise to pay for these goods and services.

**Debit card**
A banking instrument used in cash transactions. Although it may display a MasterCard or Visa logo, a debit card is not a credit card. A debit card typically withdraws funds from the cardholder’s bank account, and pays the funds to an account designated by the payee. Some debit cards have a stored value from which a payment is made. A debit card is commonly accepted as an alternative payment method to cash or check for purchase of goods or services.

**Department**
For the purposes of this policy, a department is any academic or administrative unit of the University (including student agencies, organizations, and clubs) that operates under the University’s tax identification number and whose staff members are employees or students of the University.

**EMV Chip card**
Credit cards that contain an embedded micro-chip which creates a unique code for each transaction. The chip offers added protection against fraud, because when an EMV Payment Card is used, a transaction cannot be completed without the unique code generated by the chip. EMV stands for Euro-Pay, MasterCard, Visa.

**Media**
Computers, removable electronic media, paper receipts, paper reports, answering machines, faxes and any other item that contains cardholder information.

**Merchant Account**
An account that allows a business to act as a merchant location that accepts and processes credit and debit card payments. In the context of this policy, the Office of Finance and Treasury controls merchant
accounts operating under the University’s taxpayer identification number (TIN) at a partner banking institution.

**Merchant Account Holder**
The entity that enters into an agreement with a merchant service provider for processing of credit and debit card transactions. In the context of this policy, the Office of Finance and Treasury is the University’s merchant account holder.

**Merchant Services Provider**
A bank, internet service provider, or other firm that provides services related to processing of debit and credit card transactions. The University’s merchant services provider is the financial institution that serves as a liaison between University departments and the payment card companies. In the context of this policy, the University’s banking partner is the merchant services provider.

**Merchant Location**
Any University department that operates a merchant account, by accepting credit and debit card payments.

**Penetration Tests**
A simulated attempt to hack into the University’s PCI compliant computing environment.

**PCI-DSS**
The Payment Card Industry’s Data Security Standard, or “PCI-DSS”, was created to reduce losses related to credit or debit card fraud. Five members of the payment card industry, Visa, Master Card, American Express, Discover, and JCB, banded together to develop security standards for any organization that accepts, captures, stores, transmits, or processes credit and debit card information either manually or through an automated system.

**Qualified Security Assessor (QSA)**
A person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI-DSS) compliance. QSAs also conduct vulnerability scans, penetration tests, gap analyses and provide advice to merchants related to their PCI compliant systems and processes.

**Self-Assessment Questionnaire (SAQ)**
Questionnaires developed by the payment card industry which merchants must complete in order to certify that they are processing credit or debit card transactions and storing/handling cardholder data according to PCI-DSS requirements.

**Service Provider**
A third party vendor supplying equipment, software, or services that handle or process cardholder data on behalf of the University. Examples include hosting providers, vendors providing secure gateways, managed firewalls, intrusion detection systems and other services related to PCI compliance. Entities such as telecommunications carriers that only provide communication services without access to the application layer of the communication link are excluded.
University PCI Computing Environment
Princeton University’s secure PCI Compliant network, also referred to as “The CAGE” that resides in the HPCRC. All Cardholder data that is electronically stored for any period of time by the University resides on the secure servers in the PCI Computing Environment.

Vulnerability Scan
Scan of the University’s PCI compliant computing environment that identifies potential vulnerability to security threats.

V. Procedure

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 Cash Management, and updated annually.

Individuals who handle or process credit and debit card information at Princeton University
• Must be authorized by their appropriate academic or administrative department manager, dean or director.
• 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.
• Must be familiar with, and adhere to, the University’s Information Security and Acceptable Use policies.
• Must protect cardholder information in accordance with PCI-DSS.
• Must be an employee or student or volunteer at the University
• Must pass a criminal background check.
  o 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.
  o 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.
  o Exceptions to this requirement may be granted by Cash Management 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.
University Systems and Applications containing cardholder data

- 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.

- Applications processing credit card transactions are configured so that only a System Administrator can add users to the system.

- Only individuals authorized by the Academic or Administrative Manager are added to the system by the System Administrator.

- Each authorized user has a unique account and password, and does not share their account and password with anyone.

- In instances where a single administrative account must be shared amongst authorized application admins (e.g. some sort of limitation of the application itself), a second unique form of authentication (identification) must be used (e.g. Secure token) in order to gain access to the application

- Access to and querying of the cardholder database is restricted to the database administrator

- Access to systems with cardholder data is revoked immediately if a user is terminated

- Cardholder data may not be saved, copied, or moved onto local hard drives or removable electronic media.

Methods Approved for Acceptance of Credit or Debit Cards

Credit or debit card payments may be accepted using only the following approved methods:

Card Present

- Credit card dipped or swiped through an Approved Terminal or Device

Card Not Present

- Cardholder data communicated verbally over the phone

- Cardholder data received in writing on a secure analog fax or by US Mail

- Cardholder data entered into a third party PCI-DSS-compliant payment application approved by the Office of Information Security

- Cardholder data entered into a Princeton University website with a secure PCI compliant gateway approved by the Office of Information Security

Transmission of cardholder data via End User Messaging, including E-mail, instant message, or chat is strictly prohibited.
Methods Approved for Processing of Credit or Debit Card Transactions

Computers / Terminals
Only centrally managed University owned “DeSC Standard” computers, Approved Terminals and Devices, and servers in the PCI Computing Environment, can be used to process credit or debit card transactions. Any exceptions must be approved by Office of Information Security.

- 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.

- A complete list of computers/terminals used to process credit or debit card transactions must be provided to Cash Management by each Merchant Location annually. The list must include the make, model, serial number, and location of each machine.

When using a terminal to process credit or debit card receipts.

- EMV Chip Cards must be dipped into an Approved Terminal or Device.

- Non-EMV Chip Cards may be swiped through an Approved Terminal or Device. If terminal cannot read the magnetic stripe, the card number may be keyed into the terminal.

- Terminals must be set to automatically settle daily.

- 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.

The following wireless and mobile devices are currently not approved for the acceptance and processing of credit or debit card transactions.

- Card Readers (e.g. Square and other devices) that connect to mobile phones, tablets, or other wireless devices.

- Wireless keyboards

E-Commerce
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 Cash Management and OIT, and the web server must be located in a secure environment approved by OIT, located outside of the University’s PCI Compliant Computing environment. First Data Global Payeezy Gateway should be used to capture and transmit cardholder data to the University’s payment processor. Alternative secure gateways are only permitted if they have been approved by Cash Management.

Appropriate software development practices need to be followed for the creation and maintenance of any web site 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 Cash Management for a list of current practices and/or to discuss options.
Third party applications software that accepts payment by credit card must be approved by Cash Management. Prior to implementation the Department must conduct required due diligence on the software application in conjunction with Cash Management, to ensure that the application is properly configured, and to determine how cardholder data is captured, transmitted and stored by the application.

Third party software applications should be configured to utilize First Data Global Payeezy Gateway. If the application software is not compatible with First Data Global Payeezy Gateway, another Secure Gateway may be used, but must be reviewed and approved by Cash Management.

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 Cash Management for PCI language and confidentiality provisions. All Service Provider contracts, and contract renewals executed by a department must be submitted to Cash Management.

Each year the Department must verify with Cash Management 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.

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:

- Disable inactive user accounts within 90 days.
- 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
- 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
- Require strong passwords with minimum length of at least 7 characters that contain both numeric and alphabetic characters
- Verify user identity before permitting modification to any authentication credential, such as a password reset or provisioning of new token
- Require users to re-authenticate or re-activate the session after being idle for more than 15 minutes.
- Login via remote access to applications handling cardholder data requires use of a secure token and a password
If an application requires storage of cardholder data on the University network, a Merchant Location must utilize *Princeton University’s PCI Computing Environment* to process credit or debit card transactions.

- Use of the Princeton University’s PCI Computing Environment is permitted only when a third party solution is not available, and requires written approval by the Office of Information Security and Cash Management.

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

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

- In departments where the segregation of duties is not feasible, alternative and compensating controls may be implemented to achieve the desired objectives. Please call the contact named in the header of this procedure for information on how to establish appropriate controls for your area.

- The department manager is responsible for ensuring that Cash Management is aware of any changes in personnel or job descriptions that impact the segregation of duties.

**Reconciliation of Processed Credit or Debit Card Receipts**
Credit or debit card settlements from terminal receipts or web-based reports should be reconciled against project grant statements and merchant account statements. Reconciliations must be maintained by the department and are subject to review by Cash Management.

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

---

**VI. POLICY**

*Credit Card Processing Policy for University Merchant Locations*

**VII. FORMS**

*Departmental Attestation of PCI Compliance*
VIII. CONTACT ROLES AND RESPONSIBILITIES

Cash Management
- Develops and implements policy and procedures for secure processing of credit or debit card transactions in conjunction with Office of Information Security.
- Approves and opens new merchant accounts
- Manages relationship with merchant service provider and qualified security assessor
- Approves and monitors relationships with all University providers of PCI compliant software and services
- Provides training for PCI Compliance in conjunction with the Office of Information Security
- Works with Office of Information Security to complete SAQ D on behalf of the University
- Schedules quarterly external vulnerability scans and penetration tests, coordinates testing with OIT, and attests to scope of PCI environment on behalf of the University.

Office of Information Security
- Assists in development and implementation of University policy and procedures for secure handling and processing of credit or debit card transactions.
- Ensures PCI compliant systems are used to process and store cardholder data
- Completes security assessment questionnaire SAQ D annually on behalf of the University
- Conducts monthly internal vulnerability scans of University systems that store cardholder data
- Facilitates quarterly external vulnerability scans and annual penetration tests conducted by QSA.
- Co-ordinates response to suspected or actual breach in security of credit or debit card information

Academic and Administrative Department Manager of Merchant Account Locations
- Submits application for new merchant account
- Authorize individuals in the department who process and handle credit and debit cards.
- Ensures all individuals handling cardholder data in the department are properly trained.
- Completes Departmental Attestation of PCI Compliance annually
- Reports suspected or actual breach in security of credit or debit card information to the OIT Help Desk at 258-HELP.

Individuals who process credit cards or handle cardholder data
- Accept, process, handle and store cardholder data in accordance with PCI requirements
- Complete annual PCI compliance training
- Report suspected or actual security breach to department manager

Qualified Security Assessor (QSA)
- Conducts quarterly vulnerability scans and annual penetration tests
- Provides advisory services related to PCI Compliance

Merchant Service Provider
- Processes credit and debit card transactions
- Deposits credit or debit card receipts to the University’s concentration account

**Third Party Service Providers**
- Securely process, store, and transmit cardholder information in compliance with PCI DSS requirements.
- Provides services such as but not limited to website hosting and payment processing.