Office of Finance and Treasury

**How to Securely Handle and Store Cardholder Information**

<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

Any Individual who captures, stores, transmits, or has access to credit or debit card information is responsible for protecting the information, and for destroying this cardholder data in accordance with the requirements of this procedure and the [University’s Information Security Policy](#).

Departments that have a business need to store credit or debit card data must have a documented procedure approved by Cash Management.

### 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 who supports the University’s acceptance or processing of credit or debit card payments. Common examples include technical support staff with access to computer hardware and software containing credit or debit card information, or 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 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
Individuals who capture, store, transmit, or have access to credit or debit card information are responsible for properly safeguarding the data and must comply with all requirements of this procedure and the University’s Information Security Policy to protect the integrity and privacy of such information.

Types of confidential information:
The following pieces of information are considered “confidential” within the meaning of the Information Security Policy and must be protected appropriately regardless of the storage mechanisms used (e.g., on computers, on electronic, magnetic or optical media, on paper, etc.):

- Credit or debit card number
- Credit or debit card expiration date
- Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.
- Personal identification number (PIN)
- Cardholder’s name, address and/or phone number when used in conjunction with the above fields

Destruction Requirements:
- All credit or debit card information must be destroyed as soon as it is no longer needed for legal, regulatory, or business purposes, and may not be retained for more than 90 days after the transaction is processed. In the event of a critical business need, or for legal or regulatory reasons, cardholder data needs to be retained for longer than 90 days, approval must be obtained from Cash Management.
• All physical documents that are no longer necessary must be **cross-cut shredded** using a commercially available shredding device approved by the Office of Information Security.

Applications residing in the PCI Computing Environment must securely dispose of cardholder data, in accordance with all requirements set forth in **Section 3 of SAQ D – Protect Stored Cardholder Data**. If the application cannot be configured to automatically delete cardholder data after 90 days, Departments with Applications residing in the PCI Computing Environment must manually delete stored cardholder data according to the parameters above.

**Storage Restrictions:**

• By University policy, credit and debit card information may **NOT** be stored on the hard drive of any personal computer, laptop, tablet or smartphone, on the hard drive of any computer server or network storage device, or any removable storage medium, such as DVDs, CDs, thumb drives, USB keys, etc. However, in cases where there is a compelling business need and there is no reasonable alternative, Cash Management and the Office of Information Security may grant an exception allowing a department to capture, process and/or store credit card information in the University’s PCI Computing Environment.

• 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 storage of Social Security Numbers in conjunction with credit or debit card information is strictly prohibited.** The use of social security numbers is highly restricted by University **Information Security Policy**. As such, social security numbers should never be used without the approval of the appropriate information guardian.

• Neither three- or four-digit credit or debit card validation codes (CVV2) nor Personal Identification Numbers (PIN) may ever be stored in conjunction with credit or debit card information in any form.

**Storage of and Access to Webservers, Approved Terminals and Devices and Physical Documents:**

• University webservers hosting websites that accept online payment be credit or debit card must be located in a secure environment approved by OIT, located outside of the University’s PCI Compliant Computing environment

• Point-of-sale devices must be stored in a secure location and inspected periodically for tampering and substitution.

• Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days.
• While the documents are retained, they must be stored in locked cabinets located in secured areas with access restricted to authorized individuals on a need-to-know basis.

• Keys that allow access to such containers must be immediately collected from any individual who leaves the University or whose responsibilities no longer require him or her to access such documents.

• When combination locks are used, the combination must be changed when an individual who knows the combination leaves the University or no longer requires access to perform assigned work.

• For any physical documents that contain credit or debit card information all but the last four digits of the credit or debit card number must be redacted from the document. Overwriting the credit or debit card number with a marker is not acceptable.

• No lists should be maintained that include more than the last four digits of a credit or debit card number.

• If there is a business reason that requires storage of cardholder data other than as set forth in this procedure, contact the Office of Information Security or Cash Management.

• “Media” containing cardholder information including but not limited to computers, removable electronic media, paper receipts, paper reports, faxes, and answering machines that contain cardholder should not be moved from a secure area, or distributed, without prior approval from Cash Management, and the use of secure delivery methods that log and track the Media.

Requirements for Departments with Applications in the University’s PCI Computing Environment:

• Departments with Applications residing in the University’s PCI Computing Environment must conduct a due diligence call on the Application software with Cash Management, OIT and the vendor, and document and implement procedures established by OIT and Cash Management for their Merchant Location and software application.

Sharing Restrictions and Suspected Security Breaches:

• Credit or debit card information may be shared only with individuals who have been authorized to access such data by the appropriate academic or administrative manager, dean or director.

• If a breach of credit or debit card information is suspected or has occurred, the Department Manager will immediately report the breach to the OIT Help Desk at 258-HELP.

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
- Monitors PCI compliance and co-ordinates annual University Attestation of PCI Compliance
- 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.