



# **University Policy for Accepting and Handling Credit and Debit Card Payments As of March 6, 2009**

## ***Purpose***

This document describes Princeton University's policy and procedures for the proper handling of credit and debit card transactions processed through automated systems and/or manual procedures. It is intended for:

- Any individual who accepts, captures, stores, transmits and/or processes of credit or debit card payments received for the purchase of University products and services, for contributions, etc.
- Any individual who supports any University effort to accept, capture, store, transmit and/or process credit card information, such as a technical support staff member whose role gives him or her access to computer hardware and software holding credit card information, individuals tasked with shredding credit card information, etc.

This policy and procedures are intended to ensure that credit and debit card information is handled and disposed of in a manner that satisfies the University's obligation to protect such information to the level that meets or exceeds that required by the Payment Card Industry.

Since any unauthorized exposure of credit or debit card information could subject the University to reputational damage and significant penalties, failure to comply with the policy contained within this document will be considered a serious matter.

## ***Background***

To reduce their losses due to credit 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 and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry's Data Security Standard, or "PCI-DSS."

PCI-DSS is enforced through the contracts that Princeton University, as a merchant account holder, has with our merchant bank, i.e., the financial institution that serves as a liaison between Princeton University merchants and the payment card companies. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised.

For additional information about PCI-DSS, please visit the Payment Card Industry's Web site at: <https://www.pcisecuritystandards.org>.

## *Principles*

Princeton University is committed to complying fully with the expectations specified by the Payment Card Industry in its Data Security Standard (PCI-DSS). Compliance by Princeton requires that:

1. PCI-DSS compliance is mandatory for any department that accepts, captures, stores, transmits and/or processes credit or debit card information.
2. Only authorized and properly trained individuals may accept and/or access credit or debit card information.
3. Credit and debit card payments may be accepted only using methods approved by the University IT Security Officer and the Treasurer's Office.
4. Each person who has access to credit or debit card information is responsible for protecting the information.
5. Credit and debit card information must be destroyed as soon as it is no longer necessary.
6. Departments must maintain appropriate checks and balances in the handling of credit and debit card information
7. Each department that handles credit and/or debit card information must have documented procedures for complying with this policy and PCI-DSS.
8. Suspected theft of credit or debit card information must be reported immediately to the University IT Security Officer and Public Safety.

Failure to comply with these principles, as implemented in this Policy, may result in the revocation of the ability to process credit and debit card transactions and/or could lead to disciplinary action.

The following section defines the University's standard procedures in support of the above principles.

## ***Procedures to Implement the University's Credit and Debit Card Principles***

### **1. PCI-DSS Compliance is Mandatory for any Department that Accepts, Captures, Stores, Transmits and/or Processes Credit or Debit Card Information.**

Any University department that accepts credit or debit cards as payment for goods and/or services must comply with PCI-DSS to ensure the security of cardholder information. Compliance with the requirements of this policy (as updated or amended) satisfies the elements of compliance with PCI-DSS.

### **2. Only Authorized and Properly Trained Individuals May Accept and/or Access Credit or Debit Card Information**

No individual is authorized to accept, access or support systems housing credit or debit card information until the following requirements are satisfied:

- The individual must be authorized by their appropriate Academic or Administrative Department Manager, Dean or Director to do so.
- The individual must be trained in the proper handling of credit and debit card information. Individuals who are new to the role must be trained prior to taking on their credit or debit card handling duties. Individuals whose credit or debit card handling responsibilities preceded the implementation of this policy should receive training as soon as possible. The content of the training program must be reviewed and approved by the Head University Cashier in the Operation Support Department to ensure that University objectives are met.
- The individual must acknowledge his or her understanding of this policy and must confirm his or her commitment to comply with all related University policies and procedures before he or she assumes credit and/or debit card handling duties and on an annual basis thereafter. This requirement may be satisfied by the individual physically signing the "Credit and Debit Card Security and Ethics Agreement" in Appendix A of this document, or electronically indicating his or her understanding and intent to comply with this policy in an electronic form that is signed by his or her University ID and password and that mirrors the terms of the "Credit and Debit Card Security and Ethics Agreement". Academic and Administrative Department Managers, Deans and Directors are responsible for maintaining a record of the physically or electronically signed agreements for their areas.
- In cases where the individual is tasked with taking and immediately processing over-the-counter or over-the-phone credit or debit card transactions, but has no access to lists, reports and/or storage areas where credit or debit card information is held, a criminal background check and credit check is recommended but is not mandatory.

- No individual is authorized to access any lists, reports and/or storage areas where credit or debit card information is stored in electronic, magnetic, optical and/or physical (e.g., paper) form, or to support computer systems that store or process credit or debit card information until the following additional requirements are satisfied:
  - The individual must be an employee of the University.
  - The appropriate Academic or Administrative Department Manager, Dean or Director must request that the Human Resources Department perform a criminal background check and a credit check on any prospective employee who may have access to such data. A credit and criminal background check also must be performed for prospective technical support personnel who have access to any computer system or application program that accepts, captures, stores, transmits or processes credit or debit card information.
  - In cases where either check returns outstanding issues, the appropriate Department Manager, Dean or Director will 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 credit card information.
  - The appropriate Academic or Administrative Department Manager, Dean or Director must provide the Human Resources Department with a list of positions that require background checks, and must ensure that the job description for any position that requires a background check will indicate that such a check will be performed.

### **3. Credit and Debit Card Payments May Be Accepted Only using Methods Approved by the University IT Security Officer and the Treasurer's Office**

Credit and debit card payments may only be accepted in the following manner:

- in person
- via telephone,
- via FAX,
- via physical mail (not e-mail),
- through a PCI-DSS-compliant automated system that is entirely hosted by a PCI-DSS-compliant third party organization approved by the University IT Security Officer and the Treasurer's Office,
- through an automated system that is hosted in the University data center that does not accept, capture, store, transmit or process credit or debit card information itself, but refers the customer

to a PCI-DSS-compliant system hosted by a third party organization, approved by the University IT Security Officer and the Treasurer's Office, which handles credit and debit card payments on our behalf. The third party system must not return credit card numbers, expiration dates or verification values to the University-based system.

*Note – In cases where the use of a PCI-DSS-compliant third party for the capture, storage, transmission and/or processing of credit card payments is not feasible, an exception may be requested for an automated system that handles credit or debit card information on a University-based system, but only if the system can satisfy all PCI-DSS requirements. Exceptions require written approval by the University IT Security Officer and the Treasurer's Office.*

Any department that uses a third party organization to accept, store and/or process credit or debit card information on its behalf, except for any third-party organization that already has a campus-wide agreement with the Treasurer's Office, must receive from the vendor, on an annual basis, and keep on file documentation indicating that the vendor's system and procedures have been found to be in compliance with PCI-DSS by a firm that has been authorized by the Payment Card Industry to make such an assessment. A copy of this documentation should be submitted to the University IT Security Officer.

#### **4. Each Person Who Has Access to Credit or Debit Card Information is Responsible for Protecting the Information**

Individuals who have access to credit or debit card information are responsible for properly safeguarding the data and must comply with all requirements of the University's Information Security Policy to protect the integrity and privacy of such information. This policy can be found on the Web at <http://www.princeton.edu/infosecurity>.

The following pieces of information are considered "confidential" within the meaning of the Information Security Policy and must be protected appropriately from initial capture through destruction regardless 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.
- Cardholder's name, address and/or phone number when used in conjunction with the above fields

*Special note: **The use 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 never should be used without the approval of the appropriate Information Guardian.*

Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both the customer and the merchant receipts, and on any reports that may be produced by the device.

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 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, it is strongly recommended that all but the last four digits of the credit or debit card number be physically cut out of the document. Overwriting the credit or debit card number with a marker is not acceptable since the number can still be viewed in certain circumstances.

The three- or four-digit credit or debit card validation code (CVV2) must never be captured in any form.

No lists should be maintained that include entire credit or debit card numbers without the approval of the University IT Security Officer.

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.

In cases where an Academic or Administrative Department Manager, Dean or Director is granted an exception that allows an on-campus system to accept, capture, store, transmit and/or process credit card information, the manager must ensure that the design of and all procedures associated with the application comply with the requirements listed in Appendix B of this document.

## **5. Credit and Debit Card Information Must Be Destroyed as Soon as It is No Longer Necessary**

All credit and debit card information must be destroyed as soon as it is no longer necessary, and may not be retained for more than 90 days after the transaction is processed.

All physical documents that are no longer necessary must be cross-cut shredded using a commercially available shredding device approved by the University IT Security Officer.

In cases where an Academic or Administrative Department Manager is granted an exception that allows an on-campus system to accept, capture, store, transmit and/or process credit card information, the manager must ensure that computer-based data that is no longer necessary is destroyed in the manner described in Appendix B of this document.

#### **6. Departments Must Maintain Appropriate Checks and Balances in the Handling of Credit and Debit Card Information**

Departments handling credit or debit card transactions must segregate, to the extent possible, all duties related to data processing and storage of credit and/or debit card information. A system of checks and balances should be put in place in which tasks are performed by different individuals in order to assure adequate controls. For example, the same person should not process credit or debit card transactions/refunds and perform the monthly credit and debit card reconciliation. Where staffing permits, it is strongly recommended that the responsibility for processing transactions and refunds be segregated as well.

The Department Manager or his/her designee should not handle or have access to credit and debit card transactions. He or she will verify that the original supporting detail records agree with deposits on the General Ledger Journal. Terminal or web-based reports must not be the only supporting detail record.

The Department Manager or his/her designee is responsible for ensuring that Human Resources is aware of any job description changes that are made in support of maintaining the segregation of duties.

#### **7. Each Department that Handles Credit and/or Debit Card Information Must Have Documented Procedures for Complying with this Policy and PCI-DSS.**

Each department that handles credit and debit card information must have written procedures tailored to its specific organization that are consistent with this policy and PCI-DSS. Departmental procedures should be reviewed, signed and dated by the Department Manager on an annual basis indicating compliance with the University's Credit and Debit Card Policy. These procedures also must be submitted to and approved by their Dean or Vice President, the University IT Security Officer and the Treasurer's Office.

These departmental procedures will include, but are not limited to, the following:

- Segregation of duties
- Deposits

- Reconciliation procedures
- Physical security
- Disposal
- Cash register procedures (if applicable)

Departmental procedures and controls should be reviewed by the Treasurer's Office and the University IT Security Officer.

*Note - For assistance in developing departmental procedures, contact the University IT Security Officer or the Treasurer's Office.*

### **8. Suspected Theft of Information Must Be Reported Immediately to the University IT Security Officer and Public Safety.**

Any individual who suspects the loss or theft of any materials containing cardholder data, that person must immediately notify the University IT Security Officer and Public Safety.

### ***Exceptions to Required Procedures***

It is understood that a unique situation within an individual department may require a permanent or short-term exception to one or more of the above procedures. Such an exception must satisfy ALL of the following conditions:

- It must comply with all applicable PCI-DSS requirements.
- It must be approved by the University IT Security Officer and the Vice President for Finance and Treasurer.
- In the case of a permanent exception, it must be included in a department's written procedures.
- In the case of a short-term exception, it must be restricted to specific dates or events.

***Appendix A – Credit and Debit Card Security and Ethics Certification Form***

The following page is a statement of understanding and intent to comply with the University Policy and Procedures for Accepting and Handling Credit and Debit Card Payments.

Anyone who has access to credit or debit card information must sign the form and submit it to his or her Department Manager on an annual basis.



## **Credit and Debit Card Security and Ethics Agreement**

---

**Applicable to:** Any individual who accepts, captures, stores, transmits and/or processes credit or debit card information

**Effective Date:** March 6, 2009

---

Many University departments accept credit/debit card information, such as credit/debit card numbers, expiration dates and card verification codes, from donors, purchasers of University publications and services, etc.

I recognize that this information is sensitive and valuable and that the University is contractually obligated to protect this information against its unauthorized use or disclosure in the manner defined by the Payment Card Industry's Data Security Standard, and should such information be disclosed to an unauthorized individual, the University could be subject to fines, increased credit and debit card transaction fees and/or the suspension of our credit and debit card privileges.

As an individual whose role includes the acceptance, capture, storage, transmission and/or processing of credit and/or debit card information, I agree with the following statements:

- I have read the requirements stated in the University's Policy and Procedures Accepting and Handling Credit and Debit Card Information ("Policy").
- I understand that I may only accept credit and debit card payments using methods approved by the University IT Security Officer and the Treasurer's Office.
- I understand that, as an individual who has access to credit and debit card information, I am responsible for protecting the information in the manner specified within the Policy. Further, I understand that I am also responsible for effectively protecting the credentials (IDs and passwords) and the computers that I may use to process credit or debit card transactions.
- I understand that I must destroy credit and debit card information as soon as it is no longer necessary using methods prescribed by Policy.
- I understand that in cases where I suspect that a breach of credit or debit card information has occurred, I must immediately report the breach to the University IT Security Officer and Public Safety.
- If I manage an area that handles credit card information, I understand that I must have appropriate checks and balances in the handling of credit and debit card information, and that I am responsible for having documented procedures in place for complying with Policy.
- I commit to comply with the Policy and its documented procedure, and understand that failure to comply with the above requirements may subject me to a loss of credit card handling privileges and other disciplinary measures. For employees, non-compliance could result in termination of employment.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print Name: \_\_\_\_\_

## ***Appendix B – Procedures for In-House Application Systems that have been Granted an Exception to Handle Credit or Debit Card Transactions***

In cases where an Academic or Administrative Department is granted an exception that allows an on-campus system to accept, capture, store, transmit and/or process credit card information, the Department Manager must ensure that the design of the application and all procedures associated with the application comply with the following additional requirements:

- System and network controls, approved by the University IT Security Officer, must be implemented to restrict access to authorized individuals and only on a need-to-know basis. The Department Manager is responsible for ensuring that access is immediately revoked for any individual who leaves the University or whose responsibilities no longer require him or her to access such information.
- The three- or four-digit credit or debit card validation code (CVV2) must never be captured in any form.
- Credit or debit card information that is transmitted across a network must be encrypted using a method approved by the University IT Security Officer.
- No reports should be maintained that list entire credit or debit card numbers without the approval of the University IT Security Officer.
- It is strongly recommended that only the last four characters of the credit or debit card number may be retained in a database or computer file. Retaining the entire credit or debit card number in such circumstances requires the approval of the University IT Security Officer. If such approval is granted, the following requirements apply:
  - Credit or debit card information held on Princeton University computer hard drives or on removable storage media (diskettes, CDs, DVDs, USB storage devices, etc.) must be encrypted using a method approved by the University IT Security Officer.
  - Any file containing credit or debit card information stored on electronic or magnetic media (computer hard drives, diskettes, USB storage devices, etc.) that is no longer needed must be electronically “shredded” or wiped using a commercial tool and method approved by the University IT Security Officer. Merely deleting the files is not sufficient, as common computer operating systems typically leave deleted information on such media intact.
  - No computer that has hosted a software application that accepts, captures, stores, transmits or processes credit or debit card information may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have been removed from the system and physically destroyed using a method approved by the University IT Security

- Officer. The Department Manager is responsible for establishing procedures confirming that the required hard drive removal has taken place, and that all removed hard drives are protected against theft and unauthorized access through their destruction.
- No computer that has been used to manually enter credit card information received via phone, FAX, mail, etc. into a credit card system hosted by a bank or credit card service organization may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have either been electronically wiped using a commercial disk wiping tool, or have been removed from the system and physically destroyed. In both cases, the methods used must be approved by the University IT Security Officer. The Department Manager is responsible for establishing procedures confirming that the required hard drive wiping or removal has taken place, and that all removed hard drives are protected against theft and unauthorized access through their destruction.
  - Any piece of non-magnetic/non-electronic media (e.g., CDs, DVDs) that has been used to store credit or debit card information must be cross-cut shredded before being discarded using a shredding device approved by the University IT Security Officer.

## ***Appendix C – University Business/Accounting Procedures Regarding Credit and Debit Cards***

### **General Procedures**

Any University department that wishes to accept credit or debit cards for payment must first submit a written request to the University Cashier for approval before merchant account numbers are issued.

Any or all of the following credit or debit cards may be accepted for payment:

- American Express
- Discover
- MasterCard
- Visa

### **Transaction Handling**

All credit and debit card payments received and/or processed by departments must be supported by appropriate documentation as listed below:

- All in-person payments must be supported by pre-numbered receipts, which must be in consecutive order. Voided receipts must also be maintained.
- All payments received through the mail, facsimile, or via telephone must be supported by lists prepared by the mail opener or telephone operator. List entries must not include the entire credit or debit card number. At most, they should include the last four digits of the number.

### **Reconciliation**

All credit or debit card terminals and web applications must be closed out and reconciled on a daily basis.

In addition to normal reconciliation functions, the reconciler will ensure that all transaction receipts, both processed and voided, are accounted for.

The Department Manager or his/her designee should perform, sign and date reconciliations on a regular basis, but in any case not less than monthly. Reconciliations must compare all credit and debit card payments processed using original supporting documentation, with the monthly General Ledger Journal

to assure that all deposits are properly recorded. Reconciliations must be maintained by the department and are subject to review.

Departments are responsible to assure that their cost centers have been credited by the merchant services processor or bank, i.e., the departments must reconcile transactions on their Daily Settlement Reports against their Financial Statement Reports via FMS on the Web to assure that they have received credit for all processed transactions. Reconciliations must be performed at least monthly and must be signed and dated.

### **Chargebacks**

Chargebacks are credit or debit card transactions that are returned by the Depository Bank/credit card processor or are disputed by the customer and can result in additional service fees or loss of revenue to the University.

A consumer has 90 days to dispute payment. When a dispute takes place, the bank or processor will contact the Department to obtain copies of the receipts or other documentation that substantiates the charge. The Department has a limited amount of time (usually 10 days) to respond.

If the department fails to respond by the deadline or cannot provide documentation, the bank will reverse the payment and “charge back” the Department, which will appear on the Financial Statement as a debit transaction.

Departments are responsible for ensuring that any disputes, also called “chargebacks”, are handled in a timely manner. Individuals responsible for addressing disputes must check the web-based “chargeback” systems on a daily basis to identify and to respond to consumer disputes within specified time limits (maximum 10-15 days), or funds will be debited automatically from their cost centers.

Departments are responsible for monitoring disputed charges daily and collecting funds owed after a chargeback occurs if the goods or services were provided to the consumer.

### **Policy and Procedural Changes**

The Treasurer’s Office will provide departments with updated information whenever a merchant services processor or card association announces significant policy or procedural changes. Please note that these announcements are also made on monthly Merchant Account statements.