



## **Washington University Credit and Debit Card Acceptance and Electronic Commerce Policy**

The enclosed policy has been developed to protect Washington University critical operations, partners, faculty, students, donors, staff and other customers. Compliance with this policy is mandatory. If you have any questions regarding this policy or your role in implementing it, please contact the Supervisor of Cash and Credit Operations at 314-935-7090.

Version 1.0

Approval Date:

Primary Contact: Vivian Eberhardt, Supervisor of Cash and Credit Operations

**TABLE OF CONTENTS**

<b>Executive Summary</b>	<b>3</b>
Purpose	3
Roles and Responsibilities	3
Policy Violation	4
Policy Administration	4
<b>Policy Statement</b>	<b>4</b>
Obtaining Merchant IDs	4
Compliance Responsibility	4
Securing Credit and Debit Card Data	5
Third Party Requirements	6
<b>Security Breach Response</b>	<b>6</b>
<b>Definitions</b>	<b>7</b>
<b>Useful Links and References</b>	<b>7</b>
<b>Credit and Debit Card Acceptance and Electronic Commerce Policy Acknowledgement</b>	<b>8</b>

# Executive Summary

## Purpose

As credit and debit card acceptance and electronic commerce continue to grow, the card companies (e.g. VISA, MasterCard) have established merchant requirements in order to protect cardholder data. The requirements are referred to as the PCI DSS or Payment Card Industry Data Security Standard<sup>1</sup>. Any merchant who accepts credit and debit cards as a method of payment must be compliant with the PCI DSS and certify their compliance on an annual basis.

Washington University recognizes the value of accepting credit and debit cards as payment for University goods and services. Please note the University does not accept credit or debit cards for tuition payments. This policy will detail the procedures a department must follow to become a campus merchant and explain the departments' responsibilities when choosing to accept credit or debit cards. The University has contracted with a third-party PCI DSS compliant vendor to process the University's electronic commerce transactions. This policy will explain how a department utilizes this third party vendor to process payments over the Internet.

## Roles and Responsibilities

Business units are responsible for compliance with this credit and debit card acceptance policy. Internal Audit may audit for compliance at any time. Each business unit will identify a main contact who will be the responsible party for ensuring policy compliance. Compliance requires business units to:

- Obtain merchant IDs only from the Cash and Credit Operations department at the University, [angela.werremeyer@wustl.edu](mailto:angela.werremeyer@wustl.edu)
- Set up electronic commerce capabilities through the Cash and Credit Operations department only
- Use *eTransact* for all credit and debit card transactions processed over the Internet, [www.wustl.edu/etransact](http://www.wustl.edu/etransact)
- Not authorize the use of a convenience fee without authorization from the Controller's Office
- Read and enforce the twelve requirements of the PCI DSS, including securing card data in the department
- Complete the appropriate PCI DSS questionnaire on an annual basis to certify PCI DSS compliance
- Develop remediation plans for any areas where the business unit is not PCI DSS compliant or compliant with this policy
- Review third party contracts for PCI DSS compliance
- Report potential security breaches according to the Security Breach Response referenced in this document

The Cash and Credit Operations department at the University is responsible for training the business units on the policies that must be followed when a business unit decides to accept credit and debit cards as a method of payment. Cash and Credit will set up new merchant IDs and coordinate the annual self-assessment questionnaires for submission to our merchant bank. If a business unit has requested to process e-commerce transactions, the Cash and Credit Operations department will assist them in using *eTransact*.

Vendors, partners and other third parties will be required to comply with the same security standards established for Washington University business units. All third parties accessing Washington University card processing information and networks must be PCI DSS compliant.

Contracts must contain a statement that the vendor will maintain their PCI DSS compliance and provide proof of compliance upon request.

## **Policy Violation**

Non-compliance with this policy and the requirements of the PCI DSS could lead to the exposure of sensitive cardholder data. A security breach of this nature could have serious consequences for the University including: substantial fines, legal costs, auditing costs, damage to reputation, and loss of the ability to accept credit and debit card payments.

Any Washington University employee, contractor, or other party who is involved in the acceptance of credit and debit card payments on behalf of the University or on the University's network is subject to this policy. Failure to comply with this policy will result in revocation of the business unit's ability to accept credit and debit card payments. Violation of this policy may also result in disciplinary action. Payment of fines or penalties assessed against a business unit by our merchant bank for non-compliance will be the responsibility of the business unit. These fines can be as high as \$500,000 for an individual merchant.

## **Policy Administration**

The Office of the Controller has responsibility for developing credit and debit card acceptance and electronic commerce policy. The policy has been reviewed by the PCI DSS Committee and approved for implementation. The Supervisor of Cash and Credit Operations will review this policy annually and update it when there are changes to the business standards. All policy changes are subject to review by the Office of the Controller.

## **Policy Statement**

### **Obtaining Merchant IDs**

- A business unit looking to accept credit and debit card payments on behalf of the University must contact the Cash and Credit Operations department to apply for a merchant ID<sup>2</sup> and order a credit card terminal.
- If the business unit needs to accept credit and debit cards over the Internet (e-commerce) they must contact the Cash and Credit Operations department to apply for a Merchant ID and receive guidance on how to set up their e-commerce application. Any e-commerce at the University must go through eTransact unless an exception is approved by the Controller's Office.

### **Compliance Responsibility**

- The business manager (or equivalent) of the business unit will be designated as having primary responsibility for credit and debit card and e-commerce activity in the business unit.
- This designee must sign the acknowledgement at the end of this policy indicating their understanding of the requirements of both this policy and the PCI DSS. The acknowledgement should be returned to Campus Box 1147 where it will be kept on file.
- The designee should ensure that anyone who processes or has access to card data reads, understands, and adheres to the twelve requirements of the PCI DSS. These requirements can be found at [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml). They include not storing cardholder data such as: account number, expiration date,

security code, or magnetic stripe information electronically or on paper unless following the strict PCI DSS guidelines for storing sensitive information.

- The designee responsible for the merchant ID will be required to complete the appropriate PCI DSS questionnaire on an annual basis to certify PCI DSS compliance. The Cash and Credit Operations department will coordinate the annual questionnaire and PCI DSS certification process with the designee.
- At a minimum, the Network Security Office will complete quarterly network scans on the electronic commerce merchants at the University. If these scans reveal any vulnerabilities, a report will be provided to the business unit. Non e-commerce merchants may be subject to quarterly scans based on if/how they connect to the University's network.
- The business unit designee, working with their IT specialist, will be responsible for developing remediation plans for vulnerabilities found in the quarterly scans and for any areas where the business unit is not PCI DSS compliant or compliant with this policy.

### **Securing Credit and Debit Card Data**

- Treat card information as confidential and allow access on a need-to-know basis only. Per University record retention guidelines, charge slips and statements should be retained for four years.
- When displaying credit and debit card information, only the first and/or last four digits may be displayed.
- Credit and debit card information should not be stored electronically at any time. If a business unit requires an exception to this policy, the storage of the credit and debit card information must adhere to the strict requirements of the PCI DSS. These standards include encryption and firewall security. The storage of credit and debit card information on portable devices is strictly prohibited. Portable devices include but are not limited to: thumb drives, laptops, USB flash drives, and compact discs.
- Receiving credit and debit card information via fax machine is discouraged. However, if it is required to perform University business, the fax machine must be kept in a secured location. Only those employees with a need to know should have access to that fax machine. After the transaction is processed, the fax document should be stored in a secured location or shredded.
- Sending credit and debit card information via fax machine is prohibited. Daily settlement receipts sent to the Bank Liaison via fax should have no visible cardholder identification information (e.g. account number, expiration date, name).
- The three digit security code on the back of a credit or debit card is never to be stored in any form.
- Magnetic stripe data is never to be stored in any form.
- PCI DSS 12.7 requires merchants to screen potential employees prior to hire to minimize the risk of attacks from internal sources. This screening is only required for those employees with access to multiple credit or debit card numbers at any one time. For employees functioning as cashiers who only have access to one card number at a time when facilitating a transaction, this is a recommendation only and not required. However, departments should consider background checks for those employees handling this confidential

information. Examples of screening include background, previous employment, criminal record, credit history, and reference checks.

### Third Party Requirements

The PCI Data Security Standard requires that service providers accessing cardholder data comply with the PCI DSS. Business units must contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address:

- That the third party is responsible for security of cardholder data in their possession.
- That ownership of the cardholder data belongs to the Payment Card brand, Merchant Bank, and Merchants. The third party should acknowledge that such data can only be used for assisting these parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for uses specifically required by law.
- Business continuity in the event of a major disruption, disaster, or failure.
- Termination provision that ensures that third party will continue to treat cardholder data as confidential.

### Security Breach Response

Requirement 12 of the PCI DSS states that merchants must maintain a policy addressing information security for employees and contractors. Washington University has a thorough information security policy<sup>3</sup> that should be reviewed annually by the business units. Requirement 12 also mandates the creation of a security breach response plan. The Washington University security incident response plan is as follows:

1. If a business unit suspects a security breach, they must contact the Network Security Office immediately at 935-7048 for 24x7 support. The Network Security Office will investigate the incident and assist the compromised department in limiting the exposure of data.
2. In addition to calling the phone number above, please adhere to Visa's *What to Do if Compromised*<sup>4</sup> guidelines:
  - ✓ Immediately contain and limit the exposure. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information
  - ✓ To preserve evidence, do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT)
  - ✓ Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable)
  - ✓ Preserve logs and electronic evidence and log all additional actions taken
  - ✓ If using a wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.
  - ✓ Be on "high" alert and monitor all systems with cardholder data.
3. If the suspected breach might involve credit or debit card information, the business unit must also contact the Supervisor of Cash and Credit Operations at 935-7090.

4. The Supervisor of Cash and Credit Operations will report the incident to the PCI DSS Steering Committee to determine the next course of action. Based on the findings by the Network Security Office, the PCI DSS Steering Committee will determine if other entities are required to be notified of the breach (e.g. card associations, merchant bank, cardholders, the public).
5. The Steering Committee will determine if policies or processes need to be updated to avoid a similar incident in the future.

## Definitions

- Business Unit – Any department, school, or third party conducting business on Washington University networks
- Cardholder Data – Any personal identifiable information associated with a cardholder. This includes, but is not limited to: cardholder name, card account number, expiration date, address, social security number, and Card Validation Codes (*i.e. the three digit code printed on the back of the card*)
- Electronic Commerce (e-commerce) - the buying and selling of goods or services by the transfer of funds through digital communications (e.g. via the Internet)
- Merchant – A department that accepts credit or debit cards as payment on behalf of the University
- Merchant Account – An account established by our merchant bank to process a department's credit and debit card sales and fees
- Merchant Bank – The financial institution the University uses to issue merchant accounts to departments
- Merchant ID – Number assigned to a merchant account to designate a specific merchant
- PCI DSS – Payment Card Industry Data Security Standard – A set of twelve requirements established by the card companies to protect cardholder data
- PCI DSS Steering Committee – Group responsible for directing the PCI DSS efforts at the University. Members consist of representatives from the Controller's Office, Treasury, Legal, Internal Audit, and IS&T

## Useful Links and References

- 1) Understanding the Payment Card Industry Data Security Standard:  
[http://www.cashandcredit.wustl.edu/campus\\_commerce/Navigating\\_the\\_SAQ.pdf](http://www.cashandcredit.wustl.edu/campus_commerce/Navigating_the_SAQ.pdf)
- 2) Merchant ID Application:  
[http://www.cashandcredit.wustl.edu/campus\\_commerce/Merchant\\_Application\\_Form.pdf](http://www.cashandcredit.wustl.edu/campus_commerce/Merchant_Application_Form.pdf)
- 3) Washington University Information Security Policy:  
<http://www.wustl.edu/policies/infosecurity.html>
- 4) VISA "What to Do if Compromised" Guidelines:  
[http://usa.visa.com/download/merchants/cisp\\_what\\_to\\_do\\_if\\_compromised.pdf](http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf)

# Credit and Debit Card Acceptance and Electronic Commerce Policy Acknowledgement

*Business units are responsible for compliance with this credit and debit card acceptance policy. Each business unit will identify a main contact who will be the responsible party for ensuring policy compliance.*

As the responsible party for \_\_\_\_\_,  
Business Unit/Department

I have received and reviewed a copy of the Credit and Debit Card Acceptance and Electronic Commerce Policy. I acknowledge that, as the responsible party, it is my role to ensure the following:

1. Merchant IDs are obtained only from the Cash and Credit Operations department at the University
2. Electronic commerce capabilities are set up through the Cash and Credit Operations department only
3. Ensure *eTransact* is being used for all credit and debit card transactions processed over the Internet
4. All employees with access to card data have read and understand this policy, including securing card data in the department
5. I will enforce this policy and the twelve requirements of the PCI DSS
6. The appropriate PCI DSS questionnaire is completed on an annual basis to certify PCI DSS compliance
7. Remediation plans are developed for any areas where the business unit is not PCI DSS compliant or compliant with this policy
8. Third party contracts are reviewed for PCI DSS compliance
9. Potential security breaches are reported according to the Security Breach Response referenced in this document
10. Failure to comply with this policy could result in the revocation of my business unit's ability to accept credit and debit card payments. Violation of this policy may also result in disciplinary action. Payment of fines or penalties assessed against a business unit by the University's merchant bank for non-compliance will be the responsibility of my business unit.

I have addressed and resolved any policy questions or concerns I have prior to signing this form.

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

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date