Administration and Department Credit Card Policy

Updated February 29, 2016

CONTENTS

PURPOSE

As a department that accepts payment cards on behalf of Washington University in St. Louis, it is your responsibility to prevent the loss of all customers' Personal Identifiable Information (PII) including but not limited to cardholder data used to process transactions. Failure to secure this sensitive information can result in fines and fees, loss of merchant department account, and severe damage to the Washington University in St. Louis brand; including the merchant department and the university as a whole.

PCI DSS

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

PCI DSS Compliance is partially measured by annual self-assessment questionnaires (SAQs) and quarterly external vulnerability scanning of websites and PCs that run credit and debit payments. To be PCI DSS compliant, all merchants must meet and adhere to all requirements listed in the DSS. Due to the fact that each merchant will have various options for handling payment cards, the SAQ used to attest compliance may vary but the responsibility is for compliance with the entire DSS.

SCOPE/APPLICABILITY

Business units are responsible for compliance with this credit and debit acceptance policy. Internal Audit or Cash & Credit Operations may audit for compliance at any time. Each business unit will identify the business manager, or equivalent, who will be the responsible party for ensuring compliance. Compliance requires business units to:

- Obtain merchant IDs (MIDs) only from the Cash and Credit Operations department at the University, Terminal MIDs can be obtained from the Bank Liaison and Online Processing MIDs can be obtained from the Campus Commerce Administrator
- Set up electronic commerce capabilities with approved solutions only
- Not authorize the use of convenience fees unless approval is obtained from the Controller's office via the Cash & Credit Operations department
- Understand and enforce all requirements of the PCI DSS, including securing card data within the department. Formally document the credit card process in the department including a network diagram if using e-commerce.
- Complete required Annual Self-Assessment Questionnaire (SAQ)

- Review current processing practices and create a remediation plan for any areas where the department is not PCI DSS compliant
- Staff processing credit cards are required to participate in or complete the annual training offered by the Cash & Credit Operations department in partnership with WUIT.
- Annually review and collect all third party Attestation of Compliance for PCI DSS Compliance
- Report any security breach or potential security breach according to the Incident Response Plan https://informationsecurity.wustl.edu/policies/incident-response-policy/
- In the event a merchant does not comply with the PCI DSS Compliance requirements, the merchant's right to accept credit cards for payment can be suspended until compliance is obtained. In the event compliance has been determined as unachievable the merchant's right to accept credit card payments will be revoked.

AUTHORITY

The Office of the Controller has responsibility for developing credit card acceptance and electronic commerce policies. The policy has been reviewed by the PCI DSS Committee and approved for implementation. The Manager 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.

SECURING CREDIT CARD DATA POLICY

- 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 in a locked secure location. When the retention period has ended all documents need to be destroyed with a cross cut or higher security shredder. If using an outside vendor like Shred-It, ensure that contracts state the third party is tracking and shredding in a PCI compliant manner.
- Receiving credit and debit card information via fax machine is discouraged. However, if it is required to perform University business, the fax machine should be a plain-paper machine and must be kept in a secured location; fax machines that are part of a multi-function printer should not be used to accept payment card data. Only those employees with a need to know should have access to that fax machine. After the transaction is processed, the document must be destroyed in a PCI DSS-compliant manner or, if retention is required, the cardholder data must be redacted before the document is stored. Sending credit and debit card information via fax machine to anyone other than the Bank Liaison 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, and name). Receiving credit and debit card information via email is prohibited.
- 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.

GLOSSARY

- Business Unit – Any department, school, or third party conducting business on Washington University networks
- Cardholder – Someone who owns and benefits from the use of a membership card, particularly a credit card
- 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)
- Expiration Date – The date on which a card expires and is no longer valid. The expiration date is embossed, encoded and printed on the card
- Magnetic Stripe Data – Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization
- Merchant Department – A department that accepts credit or debit cards as payment on behalf of the University
- Merchant Department Responsible Person – An individual within the merchant department who has primary authority and responsibility within that department for credit card transactions
- 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 (MID)– 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 https://www.pcisecuritystandards.org/
- 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 WUIT
- PIN/PIN Block – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message
- Primary Account Number (PAN) – Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device
- Sensitive Authentication Data – Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe data, CAV2, CVC2, CID, or CVV2 data (3 digit code on the back of the card), and PIN/PIN block.