THE UNIVERSITY OF IOWA

Merchant Services: Credit Card Policy and Security Standards

Revised: June 2016

I. Policy

University of Iowa departments that accept credit cards as a form of payment for goods and/or services must receive approval from Treasury Operations and the University Controller BEFORE purchasing, or contracting for purchase, any systems involved in processing credit card transactions. As a condition of approval, merchants must agree to comply with all requirements of the Payment Card Industry Data Security Standards (PCI-DSS), as well as the University specific controls outlined within this policy.

A. Who Should Know This Policy

Any individual with responsibilities for managing credit card transactions and those employees entrusted with handling or processing credit card information. This includes budget officers and systems managers.

II. Purpose

To establish guidelines and best practices for University entities engaging in the acceptance of credit cards. For the purpose of this policy, use of the term "credit cards" shall include the acceptance of cards bearing the logo of a credit card company, such as Visa, MasterCard, Discover, or American Express. Only those units which have received approval from Treasury Operations and the University Controller will be permitted to accept credit cards for payment of goods or services.

The ability to accept credit cards comes with **significant responsibilities to maintain cardholder security and to mitigate the risk of fraud**. The University, and all of its merchants, have a fiduciary responsibility to protect customer credit card information, and thus must adhere to the strict security requirements established by the Payment Card Industry Security Standards Council or face significant financial penalties if a breach or fraud occurs. It is also noteworthy that any compromise of cardholder information undermines public confidence in the University’s ability to maintain appropriate stewardship over entrusted confidential information. Lack of compliance in a single area of the University could jeopardize the University’s ability as a whole to accept payment cards.

III. General Responsibilities

University entities interested in accepting credit cards are strongly encouraged to evaluate the business need for this payment method.

Collegiate/Auxiliary/Administrative Budget Officers must be aware of and authorize applications for new merchant accounts within their areas of responsibility. Credit card acceptance requires significant departmental administrative effort as well as associated technical and financial costs.

IV. Merchant Responsibilities

A. Payment Card Industry Data Security Standards

The *Payment Card Industry Data Security Standards (PCI DSS)* were originally developed through a collaborative effort by the major card brands, MasterCard, Visa and others, as a set of technical and operational security requirements to protect sensitive credit card data. Today these standards are set by the PCI Security Standards Council (PCI SSC) and enforced by the payment card brands. ***These requirements MUST be followed by ALL entities that process, store or transmit cardholder data***.

The PCI Data Security Standard identifies twelve basic security requirements for cardholder transactions. *(See Appendix A)*

University of Iowa merchants are EXPLICITLY PROHIBITED from storing sensitive cardholder data on any University systems, including University servers, both local and those hosted off-site, workstations, and other locally maintained systems, including databases, file servers, spreadsheets, email, imaging systems, and paper files.

Sensitive Cardholder Data includes:

- Full Credit Card/Personal Account Numbers (PAN)
- Security Codes (CVC2, CVV2, CID)
- PIN/PIN block
- Full Magnetic Stripe Data (most egregious violation of PCI DSS)

Should a merchant experience a security breach, the University's credit card processor is authorized on behalf of the card brands to assess the merchant any fine levied by the card associations as well as the costs of forensic investigation, remediation, customer notification and re-issuance of cards.

A single merchant breach may result in the elevation of the merchant, or potentially all UI merchants' status to Level 1 (*see Appendix B for merchant level definitions****) at the discretion of the UI contracted bank. Level 1 status requires the merchant to pay for and submit to a third-party audit of the credit card processing environment. It should be noted that the University will not reimburse or share the cost of any expenses arising from the unintended exposure of cardholder data; expenses will be the responsibility of the breached merchant.***

B. Validation of Merchant Compliance

Compliance with PCI-DSS is not a single event, but a continuous, ongoing process.

Trustwave PCI Compliance Management Portal: University credit card merchants are **required to use Trustwave**, a web-based compliance validation tool used by the University to track merchant compliance with PCI DSS. Trustwave is used by each merchant to complete Self-Assessment Questionnaires (SAQ), set up network vulnerability scanning, review compliance reports, and access other valuable compliance tools.

Self-Assessment Questionnaire: Merchants are required to annually validate their compliance with PCI DSS by completing a Self-Assessment Questionnaire (SAQ) in Trustwave. There are seven different versions of the SAQ; the appropriate version varies by merchant and is determined by the method used to process credit card transactions. *(See Appendix C for processing methods and associated SAQ required)*

Attestation of Compliance: At the end of each SAQ is the “Attestation of Compliance”. Completion and retention of the Attestation self-certification provides documentation that your department has performed a PCI DSS self-assessment. ***It is best practice for this final step of the annual SAQ to be executed by the departmental budget officer.***

Vulnerability Scans: Merchants who are required to complete SAQ A_EP, B_IP, C or D must also configure Trustwave to perform Network Vulnerability Scans for any devices that are used to process, store or transmit credit card data. Scans are performed monthly and pass/fail results are displayed in Trustwave.

PCI Network: Merchants who are required to complete SAQ A_EP, B_IP, C or D must also contact the Information Security and Policy Office to configure systems to operate on the University PCI network. Systems on the PCI network will need to have explicit network access defined to allow network traffic through the PCI firewalls.

On-Site Periodic Review of Merchant Compliance: Merchants are subject to an on-site review of compliance and should be prepared to discuss their SAQ answers and how they are fulfilling the data security requirements. Reviews will be conducted by Treasury Operations in collaboration with the Information Security and Policy Office, which will periodically conduct an assessment of security controls in place to protect cardholder data when processing occurs over the University’s network. Reviews of these technology based implementations will include, but not be limited to, periodic network-based vulnerability scans.

C. Costs/Fees

Approved merchants are responsible for ALL costs associated with the equipment, setup, operations and maintenance of the merchant account.

1. The fees charged by the card brands (interchange) are typically 2.0%-2.5% of sales, and are calculated based on a variety of factors including the type of card presented by the consumer. To qualify for the best possible rate:

   - Make sure the settlement process is performed at the end of business each day (aka “Batching Out”). Note that some terminals and most software can be configured to perform this task automatically at a predetermined time of day. Settlement outside of the required time period may cause the transaction to be “downgraded” (meaning it does not qualify for a preferred rate because it is perceived as riskier).

   - Perform/require address verification for each transaction (aka “AVS”). AVS verifies the numeric portions of a cardholder’s billing address. For example, if your customer provides an address of 1847 Hawkeye Drive, Iowa City, IA 52242, AVS will confirm with the credit card company the numbers 1847 and 52242. If the information does not match, it may cause the transaction to be downgraded or even declined.

   - If possible, process card present transactions where the actual credit card is swiped rather than keyed manually.

2. PCI DSS Compliance Fees - $7/month charged directly to merchant

3. Monthly statements of credit card processing activity and associated fees are **ONLY** available online at Merchant Connect. Individuals must enroll for a user account on the website and will need specific information to register. Please contact treasury-creditcards@uiowa.edu for assistance.

V. New Merchant Accounts

It is strongly encouraged for University entities that wish to accept credit cards as a form of payment to first consult with their departmental budget officer and IT manager to determine if merchant card processing is warranted for business purposes. If the determination is to move forward with obtaining a merchant account, the entity must apply for merchant account privileges by using the ***Merchant Card Request Application***: https://edeposit.bo.uiowa.edu/merchacct/. When the request form has been approved by the budget officer responsible for the unit initiating the request, the form will be routed through Workflow to the University Controller, and possibly Chief Information Security Officer, for final approval (or denial).

Applications that have been approved by the University Controller will be forwarded to Treasury Operations, which is responsible for requesting new merchant accounts from the University’s credit card processor. **Merchants MAY NOT set up their own banking relationships** for payment card processing, and revenue received from payment card sales must be deposited into a designated University bank account.

Treasury Operations negotiates all banking and card processing relationships on behalf of the entire University, leveraging discounts based on larger volumes and internal controls that are not available at the departmental level.

Merchants will automatically be setup to accept MasterCard, Visa and Discover.

A. Preferred Methods for Credit Card Processing

There are many different methods for processing credit card transactions. Due to PCI DSS requirements there are methods that the University strongly encourages over others. Methods that are preferable include:

1. **Approved Gateways**: These are credit card processing services that can be integrated with web sites that need to collect payments.
   a. **Hosted pay page (HPP)** is a gateway that is used with a website, where customers input their personal credit card information. This method is strictly used for transactions initiated on the Internet and is preferred because a link to the HPP is embedded into the ecommerce website and transparently redirects the customer to the HPP provider's website. ***The University strongly recommends the use of the University's processor gateway solution, since it is Payment Application Data Security Standards (PA DSS) compliant and provided by the University's credit card processor***.
   b. **Authorize.net** is a vendor gateway that is approved and compliant with the PA DSS standards. It is a supported integration with the UI's credit card processor.
   c. **Payflow Pro** is a vendor gateway program that can be used to integrate a custom web form directly with the credit card processor. This method is only intended to meet specific needs, and carries additional control requirements to ensure the form is programmed securely. ***Each use must be approved by the University Chief Information Security Officer and the University Controller.***
2. **Credit Card Terminal**: This is a separate machine, commonly associated with small to medium size merchant accounts, where a card can be inserted or "swiped" to transmit data for authorization of the transaction amount, as well as manual entry for Mail Order/Telephone Order (MOTO) transactions. This method requires a separate, dedicated **PHONE** line for the transmission of data to the University's credit card processor.
3. **Virtual Terminal**: This is a web portal which functions similarly to a credit card terminal (see #2 listed above), however is accessible from any authorized university computer with a connection to the Internet. This method is primarily used for MOTO transactions**.**

The University highly recommends the use of University's processor virtual terminal solution as it is has been validated as compliant with PA DSS and is the Virtual Terminal application provided by the University's credit card processor.

Departments and units whose needs cannot be met through one of these approved methods must provide business justification for use of a third party product and obtain approval from the University Chief Information Security Officer and the University Controller before acquiring an alternative system. **A written agreement acknowledging the service provider's responsibility for the security of cardholder data will be required.** Third party vendors must provide proof of PCI DSS/PA DSS compliance.

B. Card Processing Requirements

Before any new merchant can start accepting credit cards, the merchant must meet the following requirements:

1. All persons involved with the processing, accounting and reconciliation of credit card transactions must complete the following Self-Service ICON training courses *(Self-Service->Personal->Learning and Development->My Training->Enroll in Course)*:

   a. **WCCARD** - Credit Card Policy Training

   b. **WSANS1** – UIOWA Security Awareness Training

2. PCI Compliance & Trustwave

   a. Initial SAQ must be completed no later than 3 months after receiving approval to process credit cards.

   b. For merchants that require external vulnerability scans, scans must commence no later than 3 months after approval.

3. Merchant must sign up to access monthly credit card processing statements at Merchant Connect. Statements are not mailed out to merchants.

4. eDeposit

   a. Read through eDeposit guide on how to post credit card sales and refunds to the General Ledger: https://edeposit.bo.uiowa.edu/edeposit/index.cfm?action=help

VI. Established Merchant Accounts

A. Card Processing Requirements

Merchants must meet the following on-going requirements to retain their merchant status:

1. All persons involved with the processing, accounting and reconciliation of credit card transactions must **ANNUALLY** complete the following Self-Service ICON training courses:

    a. **WCCARD** - Credit Card Policy Training

    b. **WSANS1** – UIOWA Security Awareness Training

2. Annual renewal of SAQ in Trustwave

    a. Make sure the SAQ completed is appropriate for the merchant's method of processing credit card transactions. *(Guide to SAQ selection located in Appendix C)*

    b. Attestation of compliance, which is the last requirement of the SAQ, must be signed by the merchant's departmental budget officer

3. If applicable, monitor monthly scan reports in Trustwave to ensure no vulnerabilities are discovered.

4. Non-compliant merchant accounts in Trustwave or merchants who are required to complete SAQ A_EP, B_IP, C or D and systems not on the PCI network will be given a reasonable amount of time, not to exceed 30 days, to resolve the issues that have caused the non-compliance. Merchants that have not corrected problems resulting in the non-compliant status within the allowed timeframe will be reported to the following individuals with the recommendation that merchant card processing privileges be terminated:

    a. University Chief Information Security Officer

    b. University Controller

    c. Departmental Budget Officer

B. Changes to an Established Merchant Account

Any changes to an established merchant account must be requested using the ***Merchant Card Request Application:*** ***https://edeposit.bo.uiowa.edu/merchacct/***

Examples of changes include:

- Termination of account
- Change of MFK for credit card accounts receivable
- Change of MFK for credit card debits (fees, chargebacks, negative net sales)
- Change of merchant primary contact
- Change of technology used to process credit cards, such as:

- A new or different method of accepting cards
- Purchasing new software or hardware
- Selecting a new gateway service provider

ALL merchant technology changes must be approved in advance, before purchase or use.

VII. Universal Compliance Requirements

1. NEVER store sensitive cardholder data electronically on any University computer or server, including in spreadsheets or local databases. (PCI 3.2)

2. Customer receipts, merchant receipts, and other printed materials should NEVER display the full credit card number (aka Personal Account Number (PAN)). Only the last four digits of the account number should be visible (after the transaction has been successfully processed). (PCI 3.3)

3. NEVER e-mail or transmit sensitive cardholder data via unsecured messaging or transfer protocols/technologies. (PCI 4.2)

4. Restrict access to cardholder data to individuals with a business need-to-know. (PCI 7.1)

5. ALL credit card documentation must be treated as a cash equivalent and should be kept physically secured, such as in a locked safe or filing cabinet. (PCI 9.6)

6. ALL credit card documentation no longer needed for business or legal reasons must be destroyed in such a manner that the sensitive cardholder data cannot be reconstructed. Acceptable destruction methods include cross-cut shredding, incineration, or placement in a locked “to-be-shredded” container, like those serviced by outside third-party document destruction companies. (PCI 9.8)

7. ALL employees with access to sensitive cardholder data must review this security policy prior to processing or accessing any credit card data. (PCI 12.1)

8. ALL employees with access to cardholder data MUST complete the following ICON courses prior to processing or accessing any sensitive cardholder data; and complete these courses on an annual basis thereafter. (PCI 12.1.1)
   - Credit Card Policy Training
   - Security Awareness Training

9. Immediately report suspected or confirmed security breaches to it-security@uiowa.edu or call 335-6332, as outlined by the following University policies: (PCI 12.10)
   - Policy IT-06: IT Security Incident Escalation http://itsecurity.uiowa.edu/it-security-incident-escalation
   - Policy IT-23: Computer Security Breach Notification Policy http://itsecurity.uiowa.edu/computer-security-breach-notification-policy

VIII. Important Links for Merchants

Trustwave – https://login.trustwave.com (Login Required)

Merchant Connect – https://www.merchantconnect.com/CWRWeb/displayMemberLogin.do (Login Required)

PCI Security Standards – http://www.pcisecuritystandards.org

Preparing Credit Card eDeposits – https://edeposit.bo.uiowa.edu/edeposit/index.cfm?action=help

UI Cash Handling Desktop Procedures - http://afr.fo.uiowa.edu/cash-handlling/cash-handling-deposits-policies-and-procedures

APPENDIX A: 12 PRIMARY REQUIREMENTS OF PCI DATA SECURITY STANDARDS

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Control Objectives	Requirements
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus 6. software or programsDevelop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

APPENDIX B: MERCHANT LEVELS DEFINED - COMPLIANCE VALIDATION REQUIREMENTS

Validation requirements for credit card merchants based on annual transaction volume and payment channel.

Level	Merchant Qualification Criteria (# of Transactions Processed)	Annual Reporting Requirement	External Vulnerability Scans	Implied Risk
1	>6M Visa transactions annually (all payment channels); merchants elevated to Level 1 by Visa	• Report on Compliance (ROC) by a Qualified Security Assessor (QSA) • Attestation of Compliance (AOC) form	Quarterly by an Approved Scanning Vendor (ASV)	**Highest**
2	Between 1M-6M Visa transactions annually (all channels)	• Annual SAQ • AOC	Quarterly ASV	**High**
3	20K up to 1M Visa e-commerce transactions annually	• Annual SAQ • AOC	Quarterly ASV	**Medium**
4	<20K Visa e-commerce & up to 1M Visa transactions annually (all payment channels)	• Annual SAQ (recommended)*	Quarterly ASV (if applicable)*	**Lowest**

*Compliance validation requirements set by acquirer

APPENDIX C: SAQ & TRUSTWAVE SCAN REQUIREMENTS

Merchant guide to SAQ selection and external scanning requirements.

SAQ Version	Description	No. of Questions	Scanning Required?	Processing Examples
A	e-Commerce, fully outsourced - Card Not Present	14	No	*Converge HPP or Authorize.net (iFrame or Redirect)
A_EP	e-Commerce, website can impact security of payment transaction	139	Yes	Direct Post or API e-Commerce solution
B	Standalone dial-up and cellular terminals	41	No	*Verifone Vx520 or Ingenico iCT 250
B_IP	Standalone PTS-approved terminals (IP)	83	Yes	Vx520, iCT 250 (IP connection)
C_VT	Virtual Terminals with keyboard entry	73	No	*Converge Virtual Terminal
C	Payment application connected to network (IP)	139	Yes	POS system, CHD environment segmented
D	All other merchants	326	Yes	POS system, e-Commerce collecting CHD

*Preferred method recommended by the University