Merchant Services: Credit Card Policy and Security Standards

Revised: March 2019

1. Purpose

To outline responsibilities, guidelines and best practices for University entities engaging in the acceptance of credit cards. This policy should be reviewed and known by any individual with responsibilities for managing credit card transactions and those employees entrusted with handling or processing credit card information. This includes business officers, IT support staff, and application developers.

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 (https://www.pcisecuritystandards.org/document_library). Lack of compliance in a single area of the University can result in significant fines and could jeopardize the entire University's ability to accept credit cards.

For the purpose of this policy, use of the term "credit cards" shall include all cards bearing the logo of a credit card company, such as Visa, MasterCard, Discover, or American Express.

2. Administrative Responsibilities

University of Iowa departments electing to accept credit cards as a form of payment must receive approval from their Business Officer, Treasury Operations, the University Controller, and the Information Security and Policy Office **BEFORE** purchasing, or contracting for purchase, any systems involved in processing credit card transactions. This process is completed using the **Merchant Account Application**: https://finapps.bo.uiowa.edu/MerchantAccount/.

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.

Credit card acceptance and PCI compliance requires significant departmental administrative effort as well as associated technical and financial costs. Departments must carefully weigh the benefits and costs related to credit card processing as well as the availability of IT resources.

A. Administrative Tasks: Tasks include account reconciliation and reporting, eDeposit creation, and PCI compliance.

B. Cost: Credit card expense includes both direct payment of fees and administrative effort costs. Approved merchants are responsible for ALL costs associated with the equipment, setup, operations and maintenance of the merchant account.

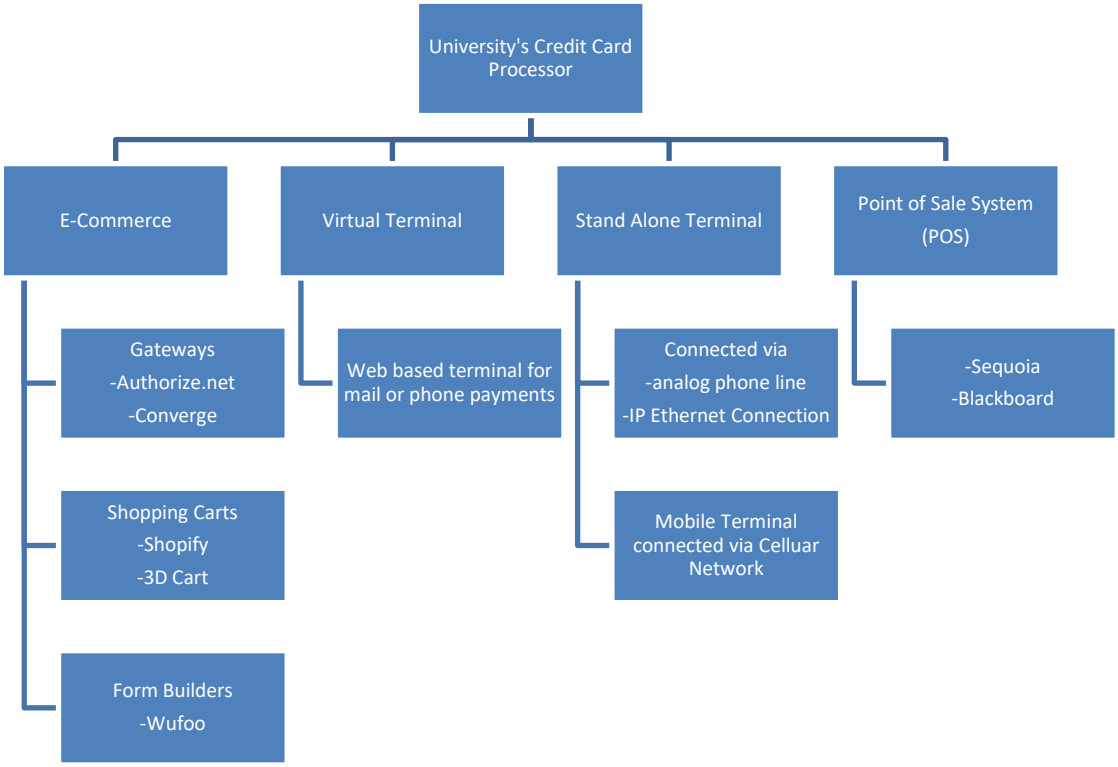
The fees charged by the card brands (interchange) are typically 2.0-2.5% of sales, and are

calculated based on a variety of factors including the type of card presented by the consumer.

C. IT Resources: Determine access and availability of local IT support and resources to assist with implementation, provide ongoing support of any Point of Sale (POS) systems or e-commerce sites, completion of PCI Matrix, as well as the required quarterly (if applicable) and annual PCI Compliance related tasks.

3. 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. Any solution utilized must be validated and approved for use by the University's centrally contracted credit card processor. Methods that are validated and approved include:



A. E-Commerce: Accepting credit card payments through a website requires the use of a Gateway for payment authorization as well as specific website requirements.

Website Requirements: E-Commerce sites must meet all requirements defined by the University's processor in order to complete merchant account onboarding. Treasury Operations will provide the list of current requirements to the unit upon approval of the Merchant Account Application. The requirements must be met to ensure receipt of revenue. *(See Appendix B)*

Approved Gateways: These are credit card processing services that can be integrated with web sites to collect payments.

1. ***Converge*** is a gateway that is used with a website, where customers input their personal credit card information. This method involves fees of $5/month and a $195 one-time setup fee. It is strictly used for transactions initiated on the Internet. This preferred method can be utilized in 2 ways:
    a) Fully outsourced ecommerce page using an iFrame or embedded link to the Hosted Payment Page (HPP) from the ecommerce website and transparently redirects the customer to the HPP provider's website. This is the preferred method of the University.
    b) University hosted website accepts or transmits the cardholder data directly and impacts the security of the payment.
2. ***Authorize.net*** is a vendor gateway that is validated with the Payment Application Data Security Standards (PA DSS). It is a supported integration with the UI's credit card processor. Monthly gateway and per transaction fees apply (https://www.authorize.net/sign-up/pricing/).

B. Credit Card Terminal: This is a standalone machine, commonly associated with small to medium size merchant accounts, where a card is present and is inserted or "swiped" to transmit data for authorization of the transaction amount, as well as occasional 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. An IP connection method is available, with approval from local IT support staff and the Information Security and Policy Office. Cellular options are available for mobile needs.

1. ***VeriFone VX520 dial up or IP terminal purchase -*** ~$495
2. ***Ingenico iWL250G Mobile Cellular terminal purchase -*** ~$749.00 + $19.00/month wireless network fee

C. 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.

D. Point of Sale System (POS): This is a system that combines cash register and credit card acceptance functions to facilitate a check out process for in person transactions. Systems must be validated as compliant with the PA DSS. Systems must be approved during the University Purchasing/Contracting process or via the Technology Review Process detailed below to ensure they will interface with the University's credit card processor and are PCI Compliant.

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 via the Technology Review Process **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. A review must be requested using the **Technology Review Process:** https://workflow.uiowa.edu/form/technology-review-form.

4. Merchant Account Responsibilities

A. Account Boarding:

Upon approval of the **Merchant Account Application**, Treasury Operations will request the new merchant account from the University's credit card processor. **Merchants MAY NOT establish their own banking relationships** for payment card processing. 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 Visa, MasterCard, Discover, and American Express.

B. Training:

All persons involved with the processing, accounting and reconciliation of credit card transactions must **ANNUALLY** complete the following Self-Service ICON training courses. (PCI 12.1.1) Units may work with their HR Unit Representative to assign these courses to all involved staff to ensure compliance is initially attained and annually maintained. *(Self-Service->Personal->Learning and Development->My Training->Enroll in Course)*:

1. **WCCARD** - Credit Card Policy Training
2. **WSANS1** – UIOWA Security Awareness Training

C. Reconciliation and Reporting

1. ***eDeposits*:** Review eDeposit downloadable guides on how to post credit card sales and refunds to the General Ledger.
2. ***Merchant Connect Reporting:*** Merchants must self-register at Merchant Connect to access monthly credit card processing statements & fees. Paper statements are not mailed to merchants. Individuals will need specific information to register. Please contact treasury-creditcards@uiowa.edu for assistance.
3. ***Monthly Reconciliation:*** Merchants must use all applicable reporting from the monthly credit card processing statements, eDeposits, POS systems, and daily batch reports to reconcile the GL on a monthly basis. https://afr.fo.uiowa.edu/policies-

procedures-resources/monthly-review-transactions-and-accounts

D. PCI Compliance Requirements

University credit card merchants, with the assistance of their designated IT support staff, are **required** to use PCI Compliance Manager, a web-based compliance validation tool used by the University to track merchant compliance with PCI DSS. PCI Compliance Manager is used by each merchant to complete an annual Self-Assessment Questionnaire (SAQ), set up external network vulnerability scanning (if applicable), review compliance reports, and access other valuable compliance tools.

In addition to guidance and direction from Treasury Operations and the Information Security and Policy Office, the University of Iowa PCI Steering Committee will provide PCI related institutional oversight for all university merchants.

1. ***Self-Assessment Questionnaire – New Merchants*:** There are eight 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 D for processing methods and associated SAQ required).* Via a collaborative effort between the department business contact and their IT Support, the initial SAQ must be completed **no later than 90 days after the onset of processing credit cards.** Merchants that have not completed this process OR 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**:
    - University Chief Information Security Officer
    - University Chief Financial Officer

2. ***Annual renewal of SAQ – All Merchants:*** PCI-DSS Compliance is not a single event, but rather a joint, continuous, ongoing process between the merchant account owner and their local IT support staff to:

    a) Ensure the SAQ completed is appropriate for the merchant's method of processing credit card transactions. *(See Appendix D)*

    b) Merchant accounts with a non-compliant SAQ and/or External Vulnerability Scan in PCI Compliance Manager, as well as 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. Non-compliant merchants beyond the allowed timeframe will be reported to the following individuals with the recommendation that merchant card processing privileges be **terminated**:

    - University Chief Information Security Officer
    - University Chief Financial Officer

3. ***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 the department has performed a PCI DSS self-assessment.

4. ***PCI Matrix:*** All merchants are required to complete a PCI Matrix during the merchant account boarding process. The PCI Matrix provides a standard template for campus merchants to document, manage, and maintain a comprehensive inventory of their PCI environment, including but not limited to, IT support staff, devices, and IP addresses of systems involved with credit card transactions. The completed PCI Matrix is expected to provide merchant support related information to facilitate business continuity and guidance of PCI compliance related activities, including timely completion of the SAQ.

5. ***PCI Network***: All Merchants required to complete SAQ A_EP, B_IP, C or D must have all applicable devices/applications/hosts, migrated, staged, and managed on the University PCI compliant network. Host migration and maintenance can be coordinated by the local IT Support staff, through the Information Security and Policy Office.

6. ***External Vulnerability Scans***: Merchants required to complete SAQ A_EP, B_IP, C or D must also configure PCI Compliance Manager to perform quarterly external vulnerability scans for all devices that are used to process, store or transmit credit card data. These quarterly scans must commence **no later than 90 days after the onset of processing credit cards**. The merchant's IT Support must schedule, review, and attest the scans each quarter.

7. ***PCI DSS Compliance Fees:*** $7/month charged directly to merchant

E. Changes to an Established Merchant Account

Any changes to an established merchant account must be requested using the **Merchant Account Application:** https://finapps.bo.uiowa.edu/MerchantAccount/.

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

Examples of changes include:

1. Termination of account
2. Change of MFK for credit card revenue
3. Change of MFK for credit card debits (fees, chargebacks)
4. Change of merchant primary contact
5. Change of technology used to process credit cards, such as:
    a) A new or different method of accepting cards
    b) Purchasing new software or hardware
    c) Selecting a new gateway service provider

F. 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 C)*

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. (PCI 3.2)

Sensitive Cardholder Data includes:

1. Full Credit Card/Personal Account Numbers (PAN)
2. Security Codes (CAV2,CVC2, CVV2, CID)
3. PIN/PIN blocks
4. Full Magnetic Stripe Data or Chip Equivalent (most egregious violation of PCI DSS)

Merchants using a shared mailbox used to communicate with customers must run Spirion scans monthly. Merchants should consult with their IT Support Consultant to provision and run the periodic scans. https://its.uiowa.edu/support/article/2697

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

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)

Any hand written credit card documentation no longer needed for business or legal reasons must be destroyed via an acceptable destruction method, including 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)

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 at the discretion of the UI contracted bank. Level 1 status requires the merchant to fund and submit to a third-party audit of the credit card processing environment by a Qualified Security Assessor (QSA). 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 (UI department/unit).

Merchants must immediately report suspected or confirmed security breaches to it-security@uiowa.edu or call 319-335-6332, as outlined by the following University policies: (PCI12.10)

1. Policy IT-06: IT Security Incident Escalation
   http://itsecurity.uiowa.edu/it-security-incident-escalation

2. Policy IT-23: Computer Security Breach Notification Policy
   http://itsecurity.uiowa.edu/computer-security-breach-notification-policy

5. Important Links for Merchants

Treasury Operations - https://treasury.fo.uiowa.edu/policies-and-procedures/credit-card-merchant-services/important-linksresources

PCI Compliance Manager – https://pcicompliancemanager.com (Login Required)

Merchant Connect – https://www.merchantconnect.com (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

IT Security & Policy Office (PCI Matrix & FAQs) - https://itsecurity.uiowa.edu/services/credit-card-handling-pci-dss-standards-compliance

APPENDIX A: BEST PRACTICES

To qualify for the best possible rate:

1. Ensure 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 an increased risk).

2. 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.

3. Whenever possible, process card present transactions by swiping the actual credit card rather than keying manually.

APPENDIX B: WEBSITE REQUIREMENTS

Merchant guide to all elements that must be present in an ecommerce website.

Requirement	Description
Merchant Name	Business (DBA) name must be clearly posted on your site. This should match the Preferred Merchant name listed on the Merchant Application.
Contact Information	Display customer service contact information including email address or phone number. This information is generally displayed in the footer of most websites.
Description of Goods & Services	Let your customers know what your website is about. Most websites have an "About Us" section to clearly define what type of business they do. This allows your customers make an informed decision regarding their purchase.
Principal Place of Business	List the merchant address, including the country name.
Display Pricing with Currency Mark	All pricing must include a dollar sign ($).
Order Page Secured	The payment page must be secure and encrypted. Self-hosted payment pages must have required security certificates.
Show Return, Refund & Cancellation Policy	This criteria can be met in one of 2 ways: 1. Show the full refund/return policy in every page leading to checkout. 2. Allow your customers a way to manually accept your return/refund policy at checkout. If Refunds or Cancellations are not allowed, that must be clearly stated.
Include Privacy Policy	Privacy Policy must be accessible and fully displayed somewhere on your website. If a department specific policy is not in place, the general UI Policy may be referenced (https://uiowa.edu/homepage/online-privacy-information).
Define Delivery Method/Timing	Indicate delivery methods & timing for products being shipped. (i.e. Standard Shipping, 2-Day Shipping, Next Day Shipping.)
Display Card Brands Accepted	Card brands require that you show the logo of the cards you accept on the payment page. This includes Visa, MasterCard, Discover, and American Express. Simply stating that you accept certain cards in text is not sufficient.

APPENDIX C: 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 software or programs 6. Develop 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 D: PCI SAQ & SCAN REQUIREMENTS

Merchant guide to SAQ selection and External Vulnerability Scan requirements.

SAQ Versi	Description	No. of Question	Scanning Required?	Processing Examples
A	e-Commerce, fully outsourced - Card Not Present	22	No	*Converge HPP or Authorize.net (iFrame or Redirect)
A_EP	e-Commerce, website can impact security of payment transaction	91	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)	82	Yes	Vx520, iCT 250 (IP connection)
C_VT	Virtual Terminals with keyboard entry	79	No	*Converge Virtual Terminal
C	Payment application connected to network (IP)	160	Yes	POS system, CHD environment segmented
P2PE	Validated P2PE payment terminals	33	No	Validated solutions listed on: https://www.pcisecuritystandards.org
D	All other merchants	329	Yes	POS system, e-Commerce collecting CHD

*Preferred method recommended by the University