Merchant Services: Credit Card Policy and Security Standards

Revised: May 2023

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 oversight, management and maintenance of credit card processing and those employees entrusted with handling or processing credit card information. This includes business officers, merchant managers, 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 Services, 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: Account reconciliation and reporting, eDeposit creation and PCI compliance tasks which include security awareness training, applicable security tasks, annual policy acknowledgement, communication of changes to an established merchant account to Treasury Services and PCI DSS Self-Assessment Questionnaire (Section 4D).

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.

C. 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.

D. **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, as well as the applicable PCI DSS Compliance related tasks required based on processing types.

3. Methods for Credit Card Processing

There are many different methods for processing credit card transactions (Credit Card Reference Guide). 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. The University maintains a list of preferred vendors and technologies that merchants are strongly encouraged to use (Credit Card Reference Guide).

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 Security Review Process **before** acquiring an alternative system. That process includes the following steps:

A. **A written agreement acknowledging the service provider's responsibility for the security of cardholder data will be required.**

B. **Third party vendors must provide proof of PCI DSS compliance as a Third-Party Service Provider that has been validated through an Onsite Assessment with a PCI QSA.**

C. **A security review must be completed using the Security Review Process:** https://itsecurity.uiowa.edu/security-review-frequently-asked-questions

4. Merchant Account Responsibilities

A. **Account Boarding:** Upon approval of the **Merchant Account Application**, Treasury Services 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 Services 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 DSS 12.6) 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->My Career->Learning and Development->My Training->Enroll in Course)*:

1. **WCCARD** - Credit Card Policy Training
2. **WSANS1 -** UIOWA Security Awareness Training
3. **WCNET1 -** UI Merchants Utilizing Transact Payments Cashnet **(for merchants using the Transact platform)**

C. Reconciliation and Reporting:

1. **eDeposits**: Review eDeposit downloadable guides on how to post credit card sales and refunds to the General Ledger.
2. **Payments Insider:** Merchants must use https://www.mypaymentsinsider.com/ to access monthly credit card processing statements & fees. Paper statements are not mailed to merchants. 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. Treasury Services and the Information Security and Policy Office (ISPO) 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 B 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 B)*

    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. **Merchant responsibilities:** All merchants are required to abide by all IT-related policies. In addition, merchants must ensure that there is a current security review on file for all applicable technology, maintain a current AOC on file for any third-party service providers, and maintain an accurate dataflow diagram on file. These requirements are maintained by Treasury Services and ISPO for merchants using the university's preferred online platform, greatly reducing the compliance burden for merchants.

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. To facilitate this support, Merchants using one of these SAQ types, must complete a simple device inventory that will be provided to the Merchants upon request from the UISO 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. *Please note*, in March of 2025, this will also apply to SAQ A Merchant accounts.

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, hardware or managed services
    c) Selecting a new 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 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. (PCI DSS 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)

NEVER e-mail or transmit sensitive cardholder data via unsecured messaging or transfer protocols/technologies. (PCI DSS 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 DSS 9.6)

Any handwritten 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 DSS 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: (PCI 12.10)

1. IT-01: Network vulnerability assessment and incident response https://itsecurity.uiowa.edu/policies-standards-guidelines/network-vulnerability-assessment-and-incident-response-policy
2. IT-18: Security https://itsecurity.uiowa.edu/policies-standards-guidelines/security-policy

5. Important Links for Merchants

Treasury Services - https://treasury.fo.uiowa.edu/credit-cards-pci-dss

Information Security and Policy Office - https://itsecurity.uiowa.edu/policies-standards-guidelines

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

Payments Insider – https://www.mypaymentsinsider.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

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 network security controls 2. Apply secure configurations to all system components
Protect account data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a vulnerability management	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement strong access control measures	7. Restrict access to system components and cardholder data by business need-to-know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an information security policy	12. Support information security with organizational policies and programs

APPENDIX B: PCI SAQ & SCAN REQUIREMENTS

Merchant guide to SAQ selection and External Vulnerability Scan requirements.

SAQ Version	Description	No. of Questions	Scanning Required?	Processing Examples
A	e-Commerce, fully outsourced - Card Not Present	22	No**	* CashNet storefront site 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	*Move5000 terminal
B_IP	Standalone PTS-approved terminals (IP)	82	Yes	*Desk3500 terminal, Desk5000 terminal
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 P2PE 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

**As of March 2025, External vulnerability scanning will be required for merchant webservers outsourcing with a third-party service provider with a URL Redirect or iFrame integration.