Credit Card Acceptance Home Page


Operating Principles:

The following operating principles and responsibilities must be used by departments when accepting credit card information in order to process payments for services, purchases, registration, etc.

1. All merchant sites must be authorized by the UWM Controller’s Office. See Application and Service Level Agreement (SLA). SLA’s must be renewed annually.
2. All merchant card services offered by the University must be delivered using software, systems, and procedures that are compliant with applicable standards.
3. UWM will pre-authorize e-Payment services for use by UWM units. (Pre-Authorized e_Payment services)
4. There should be a certain level of uniformity/branding in the look and feel of UWM storefronts except where the vendor dictates (ex. VISA has recommended standards). This uniformity not only gives institutional identity to UWM but can be used to avoid phishing.
5. Units must coordinate the delivery of goods and services with the timing of charging e-Payments to customers as defined in the credit card operating regulations.
6. The unit selling the goods or services must develop processes for handling charge card and bank account information provided by customers on paper in a safe way. Paper documents showing this information must be cross-shredded or the information must be blacked out on retained documents. Documents should be retained only for the period specified in the Records Disposal Authorization Form.
7. UWM units must reconcile e-Payments with goods and services provided and with funds deposited by the e-Payment processor into University bank accounts and into the Shared Financial System ledger. These reconciliations should be performed using the appropriate separation of duties.
Credit Card Merchant (Department) Responsibilities (agreed to in SLA):

Requirements associated with this policy apply to departments that accept credit card information for activities such as fund raising and pass it on for processing by another department, the UWM Foundation or the UWM Alumni Association.

Credit Card Merchant Numbers

a) All credit card merchant sites must be established through Controller's Office. Departments are prohibited from obtaining merchant ID numbers directly from the credit card companies.

b) Each campus merchant site must keep current, a contact person for the Controller’s Office.

Credit Card Transaction Channels

c) Credit card information can only be accepted through a UWM authorized web application or by telephone, mail, or in person.

d) Credit card information cannot be accepted or received via email, fax, instant messaging, chat, text or other end user messaging technology. Credit Card information should not be photocopied.

e) Without approval from the Controller’s Office, departments are not permitted to transmit, process, or store credit card information on UWM computer systems, fax machines, the Internet, e-mail or any removable electronic storage (USB memory stick, hard drive, zip disk, etc.); not even if encrypted.

f) If it is absolutely necessary to record the entire credit card number to process the transaction or if you receive the credit card number on paper, all but the last four digits of the credit card number must be properly destroyed immediately after processing (blackout is not a sufficient deletion method).

g) Campus networks may not be used for transmitting PCI data unless specifically authorized by Security and the Controller.

h) Merchants may not enter payment card numbers on the customers behalf in web based services designed for customer self-service.

Credit Card Information Storage

i) Without approval from the Controller’s Office, credit card merchants cannot store credit card information on a local computer or server.

j) Under no circumstances should the Card Identification Number (CID) be stored electronically or on paper after authorization. The CID number is the three digit security code on the back of the credit card. It is also referred to as the CVC2 and CVV2.

k) The electronic storage of credit card data should be limited to the amount and retention time which is required for business, legal, and/or regulatory purposes.
While waiting to be processed, paper records of the transaction, with credit card information, must be stored in a locked room or file cabinet. Access to the storage area(s) must be limited to authorized credit card personnel only.

Paper records containing credit card data must be securely destroyed at the earliest possible date while complying with relevant data retention schedules.

Credit Card Receipts

Credit card receipts that go to the customer may only show the last four digits of the credit card number. Also, the credit card expiration date must not appear on the receipt.

Retain the original receipts, which show only the last four digits of the credit card number, for all transactions and any original, signed documentation in a secure location for a minimum of 12 months as required by the University of Wisconsin System Fiscal and Accounting General Records Schedule. Ensure secure destruction of the documents after this period has elapsed.

Fees, Reconciliations, Refunds & Disputes

Departments are responsible for all credit card fees.

Reconciliation of credit card merchant activity must be performed at least monthly.

There must be adequate separation of duty between any person authorized to issue a refund and the individual reconciling the account.

Refunds must be credited to the same credit card account from which the original purchase was made.

Each department is responsible for following up and resolving disputed transactions.

Annual Self Assessment & Network Scan

Each department processing merchant cards must complete an annual risk/security questionnaire/self-assessment. As part of this self assessment, the Merchant must verify that all third party payment application software, service providers and gateways that store, process or transmit cardholder data as part of an authorization or settlement referenced in the Operating Principles #3 above, are compliant with applicable payment card requirements. This verification can be performed by:

- Application Software - Determining if the applications software is listed on the Validated Payment Applications found on the PCI website with a non-expired validation date;
- Service Providers/gateways - Determining if the service provider/gateway is listed on the Visa Global Registry of Service Providers – PCI DSS Validated Entities ( with a non-expired date.

Once completed, the questionnaire should be sent to the Controller’s Office for tracking and distribution. The Controller’s Office will then send the questionnaire to Internal Audit and the UWM Information Security Information Security Officer for follow-up.
v) For all of the third party vendors referenced in Operating Principles #3 above, the Merchant must request written acknowledgement that the service providers are responsible for the security of cardholder data that the service providers possess.

w) In addition, if credit card numbers are stored electronically, network scans must be performed quarterly by an Approved Scanning Vendor (ASV). Departments should work with UWM Information Security to have these scans performed.

x) Departments must work to resolve exceptions identified on the annual risk/security questionnaire/self assessment. Departments should work with UWM Information Security to address any exceptions pertaining to technology or electronic storage. Consult with Internal Audit as needed.

**Employees Handling Credit Card Information**

y) All employees handling cardholder data must sign a Confidentiality Acknowledgement form. The form should be the campus-wide form used by all departments.

z) All employees handling cardholder data must receive initial PCI information security training to be developed by Security and the Controller.

**Imprint Machines**

aa) Special rules will apply if imprint machines are absolutely necessary. These rules will be detailed in the SLA.

**Exceptions To These Responsibilities**

bb) While the Controller’s Office does not have the authority to override the PCI Requirements, any exceptions you have to these responsibilities should be discussed with the Controller. The Controller’s Office will consider exceptions to any of the above-stated responsibilities on a case-by-case basis in consultation with UWM Information Security and Internal Audit. In considering exceptions, the Controller’s Office will examine compliance with applicable standards and the existence and reliability of compensating controls. Departments are responsible for obtaining approval from the Controller’s Office.

**Consequences of Not Complying**

cc) If a merchant does not comply with the above responsibilities, it may be determined that the merchant will no longer be allowed to accept credit cards and may result in significant financial penalties to the department and the campus as a whole. The actions of one merchant can jeopardize all the campus merchants ability to accept credit cards.
Controller’s Office Responsibilities:

a) Promulgate standards for the campus with respect to accepting credit cards.
b) Apply for and secure all campus merchant ID numbers.
c) Establish and maintain a process for campus departments to accept credit cards.
d) Approve applications from campus departments before credit cards can be accepted.
e) Initiate and approve service level agreements with each department before credit cards can be accepted. Service level agreements will address the appropriate separation of duties within each department.
f) Reconcile monthly statements from credit card companies to the Shared Financial System.
g) Ensure credit card processing fees are properly charged in accord with state, UWS and UWM contracts.
h) Ensure credit card processing fees are properly charged back to the appropriate department.
i) Initiate annual renewals of all service level agreements between the Controller’s Office and the departments.
j) Provide appropriate training to the campus on merchant card transactions.
k) Ensure that each campus department that accepts credit cards completes the risk/security questionnaire/self-assessment required by applicable standards on an annual basis. During this annual process, the Controller will be responsible for verifying that all Merchants provide appropriate compliance documentation of all third party payment application software, service providers and gateways that store, process or transmit cardholder data as part of an authorization or settlement referenced in the Operating Principles #3 above.
l) Maintain a central file of all documentation indicating third-party vendor and third party payment application software compliance with applicable requirements.

UWM Information Security Responsibilities:

a) Work with the Controller’s Office to promulgate standards for the campus with respect to accepting credit cards.
b) When requested by the Controller’s Office, approve all applications for departments that accept credit cards.
c) Work to resolve exceptions pertaining to technology or electronic storage noted on the annual risk/security questionnaire/self-assessment and quarterly network scans. Consult with Internal Audit as needed.
d) Perform network scans required to be PCI compliant. Coordinate this effort with Internal Audit.
Internal Audit Responsibilities:

a) In the short term, Internal Audit will provide overall guidance and leadership to the campus wide credit card compliance effort.

b) Long-term, Internal Audit will turn over credit card compliance leadership to the Controller’s Office and assume a role of monitoring the continuation of the overall effort by incorporating credit card risk into the overall audit plan.

Who should know this procedure?

- Deans, Directors and staff dealing with merchant card revenue.