

The University of Iowa

Credit Card Handling Policies and Procedures

POLICY

Policy Statement

The establishment of control measures for credit card transactions is necessary to maintain proper security over credit cardholder information. The University credit card handling policy requires each unit be certified as a credit card processing merchant, and each method of processing credit transactions be approved by the University Business Office. A credit card merchant is defined as a department or other entity which processes credit transactions.

Requirements for credit card merchants include the following:

- Approval of the University Controller before entering into any contracts or purchases of software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device).
- Approval of the University Information Technology Security Office of all technology implementation, including approval of authorized payment gateways.
- Establish departmental procedures for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc.
- [Perform an annual security self-assessment](#) and report the results to Treasury Operations to ensure compliance with this policy and associated procedures.
- Compliance with [Payment Card Industry \(PCI\) Data Security Standards](#)

Periodic reviews of safeguarding and storage of cardholder information will be conducted by Treasury Operations, and credit card handling procedures are always subject to audit by Internal Audit and external audit or charge card review firms. In addition, the University Information Technology Security Office will periodically conduct an assessment of security controls in place to protect technology implementations, including but not limited to periodic network-based vulnerability scans. Departments not complying with approved safeguarding, storage and processing procedures may lose the privilege to serve as a credit card merchant.

Who Should Know This Policy

Any official or administrator with responsibilities for managing University credit card transactions, and those employees who are entrusted with handling credit cards and credit card information.

Responsibilities

Department or Unit Executive Officer - Submit a request to establish a merchant account.

Credit Card Handling Supervisor- Design an adequate process and procedure to ensure the following standards are maintained:

- Keep secure and confidential all cardholder numbers and information. Credit card receipts should typically be treated the same as you would treat large sums of cash. The department will be responsible for any losses due to poor internal or inadequate controls.
 - Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data), cannot be stored in any fashion on computers or networks.
 - Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured fax, or through campus mail (sealed envelopes may be used).
 - All documentation containing card account numbers must be maintained in a “secure” environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes.
 - All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life (18 months) has expired.
- Restrict access to credit card data and processing to appropriate and authorized personnel.
 - Background checks must be performed prior to hiring of any positions with unrestricted access to cardholder information.
 - Require all personnel involved in credit card handling to attend card security training at least every two years.
- Establish appropriate segregation of duties between credit card processing, the processing of refunds, and the reconciliation function. Supervisory approval of all card refunds is required.
- Perform an annual self assessment to ensure compliance with this policy and associated procedures, and report the results of this assessment to Treasury Operations.
- Notify the University Information Technology Security Office prior to implementation of any technology changes affecting transactions processing associated with the merchant account.

Credit Card Handlers and Processors- Agree not to disclose or acquire any information concerning a cardholder's account without the cardholder's consent. Credit card authorizations must be kept for 18 months for response to copy requests and charge-backs. E-commerce and merchants using third-party software, including cash register systems, are prohibited from storing complete payment card numbers on University computers at any time. Other (external) credit card merchants must securely store and transmit information using at least 128 bit encryption, and provide a letter to the merchant unit attesting to Payment Card Industry Data Security Standards compliance.

Controller - Review and approve the establishment of new merchant credit card processors.

Treasury Operations – Administer the process of obtaining new merchant numbers. Conduct periodic reviews of existing merchants regarding safeguarding and storage of cardholder information. Provide periodic training on the secure storage and disposal of all non-ecommerce credit card paper transaction records in conjunction with cash handling training. Provide an annual report to the University Information Technology Security Office of all merchant accounts, associated transaction volumes, and security self assessment reports.

Information Technology Security Office - Review and approve implementation of any technology changes and payment gateways associated with credit card transactions processing. Conduct periodic reviews for compliance with Payment Card Industry Data Security Standards.

PROCEDURES

Establishing New Credit Card Merchant Account

In order to accept credit cards in return for goods/services, departments (Merchants) must complete a [Payment Card Merchant Agreement](#) and return the document to the University Controller, 4 Jessup Hall. Upon approval, Treasury Operations will establish a new merchant account with an authorized merchant credit card provider. If at any time you have a question or concern about accepting credit cards, please contact Treasury Operations for assistance.

It will take approximately three weeks for merchant numbers to be requested/set up and to obtain the equipment as needed. A training session for you and your staff will then be scheduled.

Equipment & Supplies

New Merchants will be required to purchase their own equipment and supplies. One terminal/printer is required, and may be rented or purchased.

Accounting for Transactions

The daily net sales electronically settle into the appropriate University bank account designated by Treasury Operations. This information is automatically loaded into the E-deposit system daily. There is an approximately 48-hour difference from batch settlement date to receipt of funds. It is the responsibility of the Merchant to submit accounting information within three working days of the credit card batch close date through the E-deposit system. The process is described in detail on pages 11-13 of the Cashier's Office Edeposit Procedures, https://edeposit.bo.uiowa.edu/Help/Docs/edeposit_documentation.pdf

It is the Merchant's responsibility to reconcile the settlement amount in the general ledger (inst acct 1100) to the credit card receipts on a regular basis, but no less than monthly.

In addition, each Merchant receives a monthly statement directly from the authorized merchant credit card provider. These statements provide a listing of each batch submitted for reconciliation purposes. It is the Merchant's responsibility to verify that this information is correct.

Additional Information

FEES. Each transaction is subject to assessment, discount and per item fees charged by Visa and Mastercard.

Additional fees are assessed by the authorized merchant credit card provider, based on a competitive bid process. These fees include fees for transaction processing, chargebacks and supplies. Please contact Treasury Operations for current information.

Electronic commerce transactions must be processed using an authorized payment gateway and will be subject to additional costs related to this process.

PAYMENT CARD INDUSTRY GUIDELINES

[Visa Merchants Card Management Guide:](#)

[Mastercard International Rules Manual](#)

[Payment Card Industry Data Security Standard:](#)