UNIVERSITY OF MICHIGAN
FINANCE

Merchant # (Treasurer's Office Use Only): _____

The University of Michigan
Treasurer's Office
Card Services

Merchant Services Policy Document

Describe Business Purpose:

Enter Merchant Name (25 characters max):

_____

UNIVERSITY OF MICHIGAN
FINANCE

Table of Contents

Section 1: Overview

Why should you care about reading this document?

Accepting payments by credit card is very convenient and one of the most recognized methods of payment. If utilized safely, it can enhance the revenue stream of your department. By being approved to use this method, you are responsible for the associated risks of fraud and identity theft which could include the following consequences:

- Damage to reputation of your department and the entire University
- Fines
- Card re-issuance fees
- Forensic investigation costs
- Costs of notifying victims
- Remediation costs
    - External network scanning requirements
    - Network security hardware
    - Mitigation to approved applications

The Treasurer's Office supports the acceptance of credit card payments in a secure environment and wants you to be as informed as possible about the risks and business processes that support the payments.

Background

As delegated by the EVPCFO under Regental Bylaw 3.01, and detailed in the Delegation of Authority SPG 601.24 and Banking SPG 519.01, the Treasurer has overall responsibility for the administration and oversight of all banking services (including credit card services) for the University of Michigan.

The University maintains a centralized management approach for all of its Treasury Services. These responsibilities will be met through the employment of technology, timely and efficient banking practices, synergies leveraged through University wide volume and commitment to risk-averse management for funds on deposit with the University's banking partners. In order to maintain compliance to existing contracts and consistency in practice, no individual, department, school or college has the authority to establish an active bank account or enter into a Treasury Services agreement without the endorsement of the Treasurer's Office.

Process Overview

The Treasurer's Office/Merchant Services in conjunction with Financial Operations/Accounting Services provide a centralized credit card payment option to all University units. The Treasurer's Office is responsible for setting up merchant accounts, equipment and acts as the single point of contact between the bank and the University. Financial Operations/Accounting Services is responsible for the correct recording of credit card activity in the University's General Ledger. The University's credit card processor (merchant acquirer) allows departments as merchants to accept the following credit cards:

a. Visa
b. MasterCard
c. Discover (also Japan Credit Bureau (JCB) and China Union Pay (CUP) cards)
d. American Express

The University accepts card payments in a variety of methods that incorporate varying degrees of risks. The methods are outlined as follows:

1. Terminal Processing
2. Software Processing
3. Online Processing

The **Treasurer's Office website** as well as the **Standard Practice Guide 501.6** contains additional information concerning credit card policies.

Business Requirements

A Merchant is defined as a department or other entity which processes credit card transactions. Requirements for Merchants include the following:

- Approval from the Treasurer's Office before entering into any contracts or purchases of services, software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g., e-commerce, POS device).
- Demonstrated ability to maintain compliance with Payment Card Industry (PCI) Data Security Standard discussed below in this document.
- Complete an annual PCI security self-assessment questionnaire and submit results of network scans and mitigative actions to ensure compliance of this policy and associated procedures.
- Complete an online merchant certification course. The merchant contact and authorized staff are required to complete this training annually.
- Completion of this Merchant Services Policy document which is subject to annual review by each Director Level Management Authority, and changes to the Authorized Staff Roster, which should be submitted as they occur.

Section 2: Merchant Security Requirements

Before a potential merchant makes a decision to take credit cards, it must ascertain that it has the ability to comply with the PCI Data Security Standard.

IMPORTANT - **Merchants who fail to maintain compliance with the PCI Data Security Standard will have their merchant number inactivated and will no longer be able to accept credit card payments.**

In addition to the PCI security standards, proper internal controls must be in place that enhances loss prevention. Section 3.5 of this document addresses internal controls.

Payment Card Industry (PCI) Data Security Standard

Background

The Payment Card Industry (PCI) Data Security Standard is the result of collaboration between Visa and MasterCard to create common industry security requirements. Other card companies (Discover and American Express) have also endorsed the standard within their respective programs.

All Merchants must be PCI compliant and are responsible for ensuring the compliance of their unit and any third-party service providers. Merchants should require their third-party provider to sign an agreement stating that they meet PCI security standards and that the third-party provider is liable for any fines which result from a security breach. Additionally, Merchants should keep on file a valid certificate of compliance from their service provider.

These standards apply to all payment methods, including retail (brick and mortar), mail/telephone order, and e-commerce. These standards are also applicable to non-University entities that are

using University systems to process transactions. The PCI standard offers a single approach to safeguarding sensitive data for all card brands.

The PCI Data Security Standard identifies 12 basic requirements grouped into six categories.

Build and Maintain a Secure Network

1) Install and maintain a firewall configuration to protect data
2) Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3) Protect stored data
4) Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5) Use and regularly update anti-virus software
6) Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7) Restrict access to data by business need-to-know
8) Assign a unique ID to each person with computer access
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

Each merchant, including supporting IT staff and SUL (Security Unit Liason) if applicable, should be aware and comply with these standards. **The signature on this Merchant Services Policy document indicates your awareness and compliance.**

2.1 Data Security and PCI Highlights

The following are highlights of PCI that are particularly relevant to the Business Manager's decision to accept credit cards. The balance of the requirements are found in the document and are also applicable.

Ref.# - Description

1.3 Prohibit direct public access between external network and any system that stores sensitive cardholder data. Design a firewall architecture that segments credit card processing systems from all other systems.

IMPORTANT - Departments are not allowed to store electronically cardholder data on any University system. This includes, but is not limited to, computers, servers, laptops and flash drives. In very rare cases permission may be granted from the Treasurer's Office and Information and Infrastructure Assurance (IIA). If approved, merchants who intend to store cardholder data electronically will be required to have a PCI Qualified Security Assessor (QSA) annually validate their PCI compliance. Additionally, a qualified PCI penetration test will need to be performed annually. This is usually an expensive alternative for the merchant.

Do not store sensitive authentication data subsequent to authorization (even if encrypted). Do not store the full contents of any track from the magnetic stripe, expiration date, the card validation code, or personal identification number (PIN)

Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed).

IMPORTANT – The customer copy of the receipt MUST be truncated! Notify the Treasurer's Office immediately if your credit card terminal is not truncating the card number on the customer receipt.

Render sensitive cardholder data unreadable anywhere it is stored. *Credit card receipts or order forms 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.*

4.2 Never send cardholder information via unencrypted e-mail. *Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured fax, or through campus mail.*

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.

9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunications lines, paper receipts, paper reports, and faxes) that contain cardholder data.

IMPORTANT – Paper records are not allowed to contain sensitive cardholder data, this includes receipts and forms; no more than the last four digits of the credit card number can be stored. Only the Treasurer's Office can grant an exception to this policy. See the notes under Ref 1.3 regarding the policy for the electronic storage of cardholder data.

9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:
9.7.1 - Classify the media so it can be labeled as confidential.
9.7.2 - Send the media by secured courier or other delivery method that can be accurately tracked.

9.10 Destroy media containing cardholder information when it is no longer needed for business or legal reasons. *All forms of 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.*

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

12.6 Make all employees aware of the importance of cardholder information security. *The department is responsible for training and requiring the employees to acknowledge in writing that they understand the Merchant Services Policy document and that they have completed the online merchant training course.*

12.7 Screen potential employees to minimize the risk of attacks from internal sources.

12.8 Contractually require all third-party service providers with access to cardholder data to adhere to PCI security requirements. *Units that allow external vendors to process credit*

card transactions using University systems are responsible for ensuring those vendors' implementations are PCI compliant.

If a merchant wishes to process recurring transactions (section 5.12 of this manual for procedures), approval must be given by the Treasurer's Office before proceeding.

The Treasurer's Office needs to be notified prior to implementation of any technology changes affecting transaction processing associated with the merchant account.

2.2 Security Breach

A security breach is the unauthorized access of cardholder data, which includes:

- Loss
- Theft
- Fraud

An example of a breach would be the theft of credit card receipts that contain the full credit card number.

If a merchant experiences or suspects a breach of their merchant account they **MUST** immediately email all details to merchantservices@umich.edu at the Treasurer's Office.

If known, the merchant should be prepared to provide the Treasurer's Office a list of the card brands (i.e. Visa, MasterCard, AMEX, and Discover) and the credit card numbers involved in the breach.

Once notified, the Treasurer's Office will contact U-M's credit card processor. In turn they will contact the card brands affected by the breach, who in turn will contact the issuing banks. The issuing banks may decide to contact the individual cardholders.

Regardless of the actions taken by the issuing bank, the Treasurer's Office will determine if the individual cardholders are to be notified by the merchant.

Depending on the severity of the breach and exposure to cardholder data, the card brands (i.e. Visa, MasterCard, AMEX, and Discover) could assess fines to the University starting at $5,000 and escalating up to $500,000. The Merchant involved in the breach will be responsible for cost of the investigation, remediation, card re-issuance, and any and all fines (including fraudulent activity).
Merchants should also refer to the following University policies that pertain to security incidents:

Standard Practice Guide 601.25, outlines the reporting requirements for information security incidents.
Standard Practice Guide 510.1, states that the Department of Public Safety must be contacted as soon as a theft is discovered. To report a theft incident call (734) 763-1131.

Section 3: Other Merchant Responsibilities

3.1 Merchant Registration Form

To become a Merchant, a unit or organization must fill out the **Merchant Registration Form** which can be found at http://www.finance.umich.edu/treasury/merchant-services. The registration form contains contact information, merchant location, chartfields for revenue/chargebacks, chartfields for fees/equipment, equipment required and processing method desired. Also, a unit or organization must fill out Sections 7-9 of the Merchant Services Policy document and return the completed pages (pages 19-21) along with the Merchant Registration form.

3.2 Merchant Change / Termination Form

The Merchant must fill out a **Merchant Change / Termination Form** in the event of any changes in the information provided on the Merchant Registration Form. The Merchant Change/Termination Form can be found at http://www.finance.umich.edu/treasury/merchant-services.

3.3 Merchant Equipment & Supplies

New Merchants will be required to purchase their own equipment. One terminal/printer is required and one imprinter if the Merchant will be handling "card present" transactions**. Please note that an analog phone line is required for electronic merchant terminals (they will not work on digital phone lines).** Terminal pricing may be found at the Treasurer's Office Web site: http://www.finance.umich.edu/treasury/merchant-services.

Due to changes in technology as well as new banking requirements, merchants should expect that they will need to replace their terminals every three years. If you experience problems with your equipment, please contact the Treasurer's Office. We will assess the problem and if necessary replace the equipment.

Supply Order Forms – for paper and thermal rolls - may be found at the Treasurer's Office Web site: http://www.finance.umich.edu/treasury/merchant-services . Please make sure to have replacement supplies on hand. The cost of supplies is included as part of our discount rate. However, merchants are responsible for shipping costs.

If you should decide to discontinue accepting credit card payments or switch your processing method (PC or online), **return your terminal to the Treasurer's Office for proper disposition**.

3.4 Merchant Certification

All Merchant staff who will be involved in processing credit cards are required to annually complete an online Merchant Certification course. The course will take on average 45 minutes to complete, and covers a number of topics including: PCI, Internal Controls and Reconciliation.

New merchants need to complete the online training prior to accepting credit cards payments.

To register for the course visit MyLINC (http://maislinc.umich.edu) and search for the course ID: TME102.

3.5 Internal Controls - Authorized Staff and Segregation of Duties

Internal controls provide important benefits to your department and to the University as a whole by improving the quality of accounting information, and it reduces the possibility of mismanagement, error and fraud. Segregation of duties is the cornerstone of internal control. It is a coordinated system of checks and balances in which tasks necessary to complete a transaction either are performed by different individuals, two or more individuals working in tandem, or the tasks are independently reviewed. No one individual should control all aspects of processing a credit card transaction or refund (i.e., reviewing daily batches, reconciling the Statement of Activity and Monthly Merchant Statement from U-M's credit card processor).

Departments should prepare a written internal control plan. An internal control plan is a description of how a department expects to meet its various goals and objectives by using policies and procedures to minimize the risks. Documenting policies and procedures will clearly communicate specific responsibilities to individual staff, facilitate training new staff, and enable departments to review and monitor their internal control system.

As a security precaution, Merchants must specify in writing to the Treasurer's Office/Merchant Services (**Merchant Services Policy document Section 7: Contacts**) the individual (s) who will be allowed to approve a Credit (Refund) Slip. **This cannot be the same person who processes sales transactions. Supervisory approval of all credit refunds is required.** ***Be aware that common fraud is for employees to process credits to their own credit card accounts.***

Each Merchant must keep a copy of this Merchant Services Policy document on file, as well as a roster of all staff members who are authorized to handle credit card transactions. The Merchant Director Level Management Authority must keep individual signatures on file from these staff members indicating they have read and understand the Merchant policies that apply to their department (refer to PCI 12.6).

3.6 Accounting for Transactions

The daily net sales are electronically settled into the appropriate University bank account designated by the Treasurer's Office. This information is automatically loaded into the General Ledger daily. The revenue will flow into the chartfields that were provided when the merchant account was set up. If at any time, the merchant wishes to change their chartfields, they should complete the Change/Termination form located at http://www.finance.umich.edu/treasury/merchant-services. There is an approximate 24-hour difference from batch settlement date to receipt of funds (excluding American Express transactions).

It is the responsibility of the Merchant to "batch out" and transmit the totals to the bank daily. **The card brands will charge a surcharge for transactions that are not batched out daily.** It is the Merchant's responsibility to reconcile the settlement amount to the credit card receipts on a regular basis, and to reconcile with the Statement of Activity on a monthly basis.

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

3.7 Daily Sales Reconciliation

The Merchant must reconcile their daily sales:

1. to the report generated when the terminal is batched out;
2. to the monthly statement provided by the Merchant Acquirer or the website information;
3. to the PeopleSoft monthly Statement of Activity.

Problems or discrepancies should be reported immediately to Financial Operations/Accounting Services at (734) 647-3767.

3.8 Notification of Change

Merchants must notify the Treasurer's Office/Merchant Services prior to making any changes to their method of processing after the merchant has been initially set up. Examples include changing from terminal based processing to processing through PC software, through a website (e-commerce), terminals built into cash registers, touch tone phone authorization, or processing through a lockbox. ***The Treasurer's Office/Merchant Services must approve all such changes prior to implementation.***

3.9 Termination of Service

If a Merchant no longer wishes to accept credit cards, the Merchant must complete the Merchant Change/Termination Form and return it to the Treasurer's Office/Merchant Services. The Merchant Change/Termination Form can be found at http://www.finance.umich.edu/treasury/merchant-services. If you should decide to discontinue accepting credit card payments or switch your processing method (PC or online), **return your terminal to the Treasurer's Office for proper disposition**. The merchant is responsible for cancelling any agreements with third party processors.

3.10 Best Practices for Card Present Transactions

Sometimes when you swipe the card, the terminal is not able to read the magnetic stripe and perform an electronic authorization. In this situation, you may need to key-enter the transaction data. When transactions are key-entered, special security information benefits are not available. Disadvantages of a key-entered transaction are 1) increased risk of fraud and counterfeit; 2) key-entered transactions cost more to process, and are declined more often; and 3) key-entered transactions are more time-consuming and allow more potential for error.

If a card won't read when swiped: 1) take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way; 2) make sure to imprint the card on the transaction receipt as this will prove that the card was present in case of a dispute; and 3) put in customer billing address and zip when prompted by terminal.

3.11 Card Validation Code (e.g. CVC2/CVV2/CID data)

Merchants may not store - under ANY circumstances - the card validation code after processing a transaction.

The card validation code was developed as an extra measure to curtail fraud for card not present transactions by the card brands (Visa, MC, AMEX & Discover). Capturing this information as part of processing the transaction may assist merchants in dealing with disputed charges (i.e. chargebacks). However, merchants must be aware that they **CANNOT** store the card validation code after processing the transaction, since this is a violation of PCI guidelines.

For this reason, Merchants may decide to create a departmental policy for when they will capture this information. For example, if the amount of the transaction is over a predetermined dollar amount, then the department may feel that the card validation code should be captured. On the other hand, for small transactions the merchant may feel that the risk of capturing the code is higher than the risk of a chargeback.

Under most circumstances it is the merchant's discretion whether to capture the card validation code. However, there are some issuing banks that require the code to process the transaction. This is especially true for cards issued by credit unions.

3.12 E-Commerce / Credit Card Processing Software

Please consult the Treasurer's Office/Mercant Services before completing the Internet Merchant Registration Form (located at http://www.finance.umich.edu/treasury/merchant-services) and before signing a contract/agreement with a Gateway provider (e.g., PayPal, Authorize.Net and Cybersource) or selecting credit card processing software.

3.12.1 E-Commerce

Prior approval from the Treasurer's Office is required **before** the Merchant selects a payment gateway for e-commerce transactions. The Treasurer's Office needs to verify that the third-party gateway service provider is PCI compliant and is compatible with our processing company (TSYS). The payment gateway vendor usually charges a merchant set-up fee, monthly gateway fee, and a transaction fee. In addition, website design and set-up (storefront) is the responsibility of the University merchant.

Departments are not allowed to capture, store, transmit, or process credit card data on University computers (e.g. servers, websites), without prior approval of the Treasurer's Office and Information and Infrastructure Assurance (IIA). Additionally, merchants who intend to store cardholder data electronically will need to have a PCI Qualified Security Assessor (QSA) annually validate their compliance and a qualified PCI penetration test performed annually. All e-commerce sites should redirect the user to a PCI compliant gateway provider to carry out the credit card transaction. Please refer to the "**IT Credit Card Policy Supplement**" (http://www.finance.umich.edu/treasury/merchant-services) for a more comprehensive explanation of this policy.

Agreements with third parties that handle credit card information on behalf of the merchant should state that the third party will:

1. Maintain compliance with the PCI Data Security Standard for the life of the contract.
2. Protect the credit card data in accordance with the PCI Data Security Standard.
3. Acknowledge responsibility for the security of the cardholder data. If a breach occurs and they are deemed responsible for the breach, they should pay all costs associated with the breach.
4. Appear on Visa's list of PCI DSS compliant service providers, located on Visa's website (www.visa.com/cisp).

Additionally, merchants should keep on file a valid certificate of compliance from their service provider.

3.12.2 Credit Card Processing Software

Prior approval from the Treasurer's Office is required before a Merchant selects credit card processing software. The software must be PA-DSS compliant and the merchant will need to provide the name of the software and version number to the Treasurer's Office. The Treasurer's Office will need to verify that the software is compatible with our processing company (TSYS).

The merchant will be responsible for ensuring that the software, and its implementation, is compliant with PCI DSS.

Please refer to the **"IT Credit Card Policy Supplement"** for additional merchant responsibilities.

3.13 P-Cards

Merchants are allowed to accept Purchasing Cards (P-Cards) from organizations not affiliated with the University. However, they should not process University of Michigan issued P-Cards. For additional information regarding P-Card policies please contact Procurement Services.

Section 4: Administrative Responsibilities

4.1 Treasurer's Office / Merchant Services

4.1.1 New Merchant Application

The completed application will be reviewed by the Treasurer's Office/Merchant Services for appropriateness and then forwarded to the Merchant Acquirer. The Merchant Acquirer will set up the new merchant account, assign a merchant number, send out the required equipment, instructions for its use and contact information for Customer Support and supplies. The Treasurer's Office/Merchant Services will also set up the new merchant in the M-Pathways system.

4.1.2 Processing Methods

If a department wishes to use a processing method other than a dial-out terminal, the Treasurer's Office/Merchant Services will assist the department on an individual basis. The processing method must be consistent with the requirements of the credit card processor, the Treasurer's Office, IIA, Financial Operations and University Audits.

4.2 Financial Operations / Transaction Services

4.2.1 Cash Receipts

Financial Operations is responsible for ensuring daily cash receipts will be generated and recorded in the General Ledger via an electronic file received from the Merchant Acquirer. Financial Operations is also responsible for ensuring all appropriate fees are charged to the merchants on a monthly basis.

4.2.2 Discrepancy Handling

Financial Operations will research and correct problems when cash receipts are not created for amounts that are consistent with the merchant's credit card sales.

Section 5: Bank Card Merchant Rules & Regulations

The following are excerpts from the "Bank Card Merchant Rules and Regulations" supplied to Treasury/Merchant Services by U-M's credit card processing bank. All merchants accepting credit cards for payments of any kind are bound by these rules and regulations. The "Bank Card Merchant Rules and Regulations" in its entirety, may be found at the http://www.finance.umich.edu/treasury/merchant-services.

5.1 Honoring of Cards

5.1.1 Non-Discrimination

The merchant shall promptly and without discrimination honor all valid Cards when properly presented as payment from Cardholders for the purchase of goods and/or services. The merchant shall maintain a policy that shall not discriminate among customers seeking to make purchases through use of a valid Card. An unreadable magnetic stripe, in and of itself, does not deem a Card invalid.

5.1.2 Transaction Amount

The merchant **shall not** establish minimum or maximum sales transaction amounts as a condition for honoring a Card.

5.1.3 Surcharges

The merchant **shall not** impose any surcharge on sales transactions.

5.1.4 Purchase Price

Any purchase price advertised or otherwise disclosed by the merchant must be the price available when payment is made with a Card.

5.1.5 Tax

Any tax required to be collected by the merchant must be included in the total transaction amount and not collected separately in cash.

5.1.6 Signature Validation

The merchant shall validate all cards by ensuring the signature on the back of the Card matches the signature on the transaction receipt.

5.1.7 Multiple Signatures

The merchant shall not accept any Card having two signatures on the signature panel located on the back of the Card.

5.1.8 Personal Information

The merchant shall not impose a requirement on Cardholders to provide any personal information, such as a (i) home or business telephone number, (ii) home or business address, (iii) driver's license number, (iv) photocopy of a driver's license or (v) photocopy of the Card, as a condition for honoring a Card unless such information is required (a) for mail order, telephone order, or delayed delivery transactions; (b) the transaction amount exceeds a pre-determined dollar limit; or (c) the information is required by the Card issuer. Except for the specific circumstances cited above, the merchant shall not refuse to complete a sales transaction solely because a Cardholder who has complied with all of the conditions for presentment of a Card at the point-of-sale refuses to provide such additional personal information.

5.1.9 Waivers

The merchant shall not require a Cardholder, as a condition for honoring a Card, to sign a statement that in any way states or implies that the Cardholder waives any rights to dispute the transaction with the Card issuer or otherwise.

5.2 Use of Service Marks

The merchant shall adequately display, in accordance with the Visa and MasterCard Rules, the Visa and MasterCard service marks, as applicable, on promotional materials to inform the public which Cards will be honored at the merchant's place of business. At a minimum, the Visa and MasterCard service marks should be on display near the entrance of the merchant's place of business and must not be less prominent than other service marks that the merchant has on display (e.g., American Express, Discover).

5.3 Authorization

The merchant shall obtain authorization for each sales transaction for the total amount of such transaction. For sales transactions not processed through an electronic terminal, the merchant shall type or print legibly on the sales draft the authorization approval code evidencing the authorization so obtained.

5.4 Verification and Recovery of Cards

If a transaction is not authorized, the merchant must not complete the sale, and, if instructed by the Designated Authorization Center to pick-up the Card, the merchant should do so by reasonable and peaceful means, notify the Designated Authorization Center when the Card has been recovered, and ask for further instructions.

5.5 Electronic Processing Merchants

Any merchant processing sales transactions through the use of an electronic terminal must comply with the following additional requirements in order to properly process sales transactions and to attempt to qualify for a reduced rate:

a. The Card must be swiped through the terminal (except for mail order or telephone order transactions).
b. If the Card account number is not electronically read from the Card's magnetic stripe, the merchant must obtain an imprint of the Card.
c. The draft with the imprint of the Card must be signed by the Cardholder and shall include the date, time, authorization code, location, and dollar amount on the same side as the imprint of the Card.

5.6 Returned Merchandise and Adjustments

A merchant shall not process a credit transaction without having (i) completed a previous purchase transaction with the same Cardholder and **the same Card** and (ii) paid related fees associated with such transaction to the Merchant Acquirer. The refund or adjustment indicated on the credit draft shall not exceed the original transaction amount.

Do not provide cash refunds for returned merchandise originally purchased with a credit card. The card associations do not permit cash refunds for any credit or debit card transaction. By issuing credits, you protect your customers from individuals who might fraudulently make a purchase on the customer's credit card account and then return the merchandise for cash.

If the original credit card is no longer available (e.g. expired, account closed) the refund may be applied to another card or by check. As with refunds, supervisory approval is required and

merchant must have a formalized process in place for tracking such activity. The Treasurer's Office has created a form to assist merchants, which is available on the Treasurer's Office Web site.

If a transaction was conducted with a prepaid card (Visa or MasterCard gift card) and the cardholder is returning items, but has discarded this card, you may give a cash refund or in-store credit.

5.7 Delivery of Sales Drafts and Credit Drafts

5.7.1 Cardholder Copy

The merchant shall deliver to the Cardholder a true and completed copy of the sales draft evidencing a transaction involving use of a Card. Such copy shall be delivered at the time of the delivery of the goods and/or performance of the services covered thereby, or for transactions initiated at point-of-transaction terminals, at the time of the transaction. The merchant shall deliver to the Cardholder a true and complete copy of each applicable credit draft at the time of the transaction, giving rise thereto.

5.7.2 Cardholder Signature

The Cardholder shall not be required to sign a sales draft until the final transaction amount is known and indicated in the "total" column.

5.8 Date and Identification

The merchant must date each sales draft and/or transaction record resulting from the use of a Card with the transaction date and should include thereon a brief description of the merchandise and/or services sold and the price thereof (including any applicable taxes) in detail sufficient to identify the transaction. The merchant must also date each credit draft resulting from the use of a Card with the transaction date and should include thereon a brief description of the merchandise returned, services cancelled or adjustment made and the amount of the credit in sufficient detail to identify the transaction.

5.9 Disclosure and Storage of Cardholder Information

5.9.1 Information Disclosure

The merchant shall not disclose a Cardholder's account information or any other personal information to third parties other than to the merchant's agent(s) for the sole purpose of assisting such merchant in completing the transaction or as specifically required by law. Suspicious requests for account information should be reported immediately to the Treasurer's Office/Merchant Services.

5.9.2 Data Retention

Credit card **account numbers** may not be stored in electronic format without the expressed, written consent of the Treasurer's Office. It is never acceptable to store the **card validation code**, (which consists of the last three digits printed on the signature panel of a Visa or MasterCard) subsequent to transaction authorization, whether encrypted or unencrypted. In keeping with the PCI Data Security Standard 3.4, render primary account numbers, at a minimum, unreadable anywhere they are stored (the first six and last four digits are the maximum number of digits to be displayed). If for some reason, a department is unable to encrypt cardholder data, they must provide the Treasurer's Office with compensating controls.

The merchant or any agent of the merchant shall not retain or store **magnetic stripe data** subsequent to the authorization of a sales transaction (even if encrypted).

The merchant agrees to retain legible copies of all sales drafts for up to 18 months in order to satisfy any disputes/chargebacks. After the 18 month period is up, the sales drafts should be shredded in order to protect cardholder information (refer to PCI 9.1).

5.10 Mail Order, Telephone Order, Delayed Delivery, E-Commerce and Recurring Transactions

The merchant may not engage in mail order, telephone order, delayed delivery, e-commerce and/or recurring transactions unless previously indicated on the merchant application. The merchant assumes all risk associated with accepting mail order, telephone order, delayed delivery, e-commerce and recurring transactions, including, but not limited to, fraudulent sales transactions.

5.11 Fees

The merchant shall be responsible for the payment of any and all transaction fees for each card transaction they conduct. The Treasurer's Office/Merchant Services reserves the right to assess an additional administrative fee to offset the administrative costs of the Merchant Program.

5.12 Recurring Transactions

If a merchant wishes to process recurring transactions, approval must be given by the Treasurer's Office before proceeding.

If a merchant agrees to accept a recurring transaction from a Cardholder for the purchase of goods and/or services which are delivered or performed periodically, the Cardholder must complete and deliver to the merchant an order form containing a written request for such goods and/or services to be charged to the Cardholder's account. The order form must at least specify:

1) the transaction amount charged to the Cardholder's account;
2) the frequency of the recurring charges; and
3) the duration of time for which such Cardholder permission is granted.

In the event that a recurring transaction is renewed, the Cardholder must complete and deliver to the merchant a subsequent order form for continuation of such goods and/or services to be charged to the Cardholder's account. A recurring transaction may include the payment of recurring charges such as insurance premiums, subscriptions, membership fees, tuition.

a. If the recurring transactions are to be for varying amounts, the following additional conditions apply:

   1) The order form must allow space for the Cardholder to specify a minimum and maximum transaction amount to be charged periodically to the Cardholder's account.

   2) The merchant must inform the Cardholder of the Cardholder's right to receive, at least 10 days prior to each scheduled transaction date, written notification of the amount and date of the next charge.

b. A copy of the order form must be 1) retained by the merchant for the duration of the recurring charges; and 2) provided in response to an issuer's request for the original sales draft.

c. Notwithstanding anything to the contrary in any agreement between the merchant and a Cardholder, the merchant shall not complete an initial or subsequent recurring

transaction after receiving a cancellation notice from the Cardholder or a response that the Card is not to be honored.

Section 6: Appendix

6.1 Definitions:

Acceptable Credit Card Companies – MasterCard, Visa, Discover (JCB & CUP) and American Express.

Authority to issue Credits (Refunds) – Departments must specify in writing to the Treasurer's Office the individual(s) that will be allowed to approve a Credit (Refund). **Supervisory approval of all credit refunds is required.**

Authorization Fees – A fee charged by the Merchant Acquirer for handling Discover and/or American Express transactions. This fee is not related to discount fees.

Card Validation Value or Code – Data elements on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:
• CAV Card Authentication Value (JCB payment cards)
• CVC Card Validation Code (MasterCard payment cards)
• CVV Card Verification Value (Visa and Discover payment cards)
• CSC Card Security Code (American Express)

The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:
• CID Card Identification Number (American Express and Discover payment cards)
• CAV2 Card Authentication Value 2 (JCB payment cards)
• CVC2 Card Validation Code 2 (MasterCard payment cards)
• CVV2 Card Verification Value 2 (Visa payment cards)

Chargeback Fees – If a customer disputes a sales transaction with the card issuer, the merchant will receive paperwork requiring them to respond within a specific period of time showing proof of cardholder authorization for that transaction. If the merchant does not respond timely, the customer will be issued a credit on their card and the merchant will be debited the disputed amount.

Discount Fees – Fees charged by acceptable credit card companies to merchants for each credit card transaction.

E-Commerce – Web based (Internet) credit card transactions.

Electronic Ticket Capture – The transmission of sales to a credit card processor through the use of electronic equipment. Credit card terminals are the most common devices used for this purpose. Other options for processing include software to allow batch processing, Web processing, and cash registers with a built-in terminal.

Imprinter – A piece of equipment used to imprint a credit card on a credit card form.
Merchant – A University school, college, department or unit that accepts credit card payments from internal and/or external customers.

Merchant Acquirer Processor – A bank or its affiliate that provides services for processing credit card transactions.

PCI DSS – Payment Card Industry Data Security Standard adopted by Visa and MasterCard to protect cardholder data. The security standard require each merchant to annually fill out a Self-Assessment Questionnaire and the Unit Director signs the document certifying its accuracy. Compliance is mandatory for University merchants.

UNIVERSITY OF MICHIGAN
FINANCE

Section 7: Contact – Treasurer's Office

Email: merchantservices@umich.edu
Phone: (734) 763-1299
Fax: (734) 763-2201

Credit Card Merchant "Contact" (Required - Business Manager/Administrative Manager)

The Department "Credit Card Merchant Contact" is responsible for the training of their individual staff in accordance with this Merchant Services Policy document.

Name:
Title:
Signature:
Email:
Phone:
Fax:

Credit Card Merchant individual authorized to sign on returned sales or credits **(Required - must be different from the person processing charge sales)**:

Name:
Title:
Signature:
Email:
Phone:
Fax:

Section 8: Authorized Staff

The merchant contact is responsible for maintaining a current listing of all individuals who are authorized to be involved in the credit card process in M-Pathways Financials and Physical Resources System (FINPROD).

An authorized user is anyone who comes into contact with or handles cardholder data (i.e., the full '16 digit' credit card number) or issues credit card refunds.

The Treasurer's Office will request FINPROD access for the merchant contact.

Use link below to obtain instructions on how to update authorize users.

https://maislinc.umich.edu/mais/html/GL_CR_Deposit_Merchant.html

UNIVERSITY OF MICHIGAN
FINANCE

Section 9: Additional Signatures

The undersigned agree to follow the rules and regulations stated in this Merchant Services Policy document. Any deviations may result in termination of ***Department*** as a credit card processing merchant. The Department "Credit Card Merchant Contact" is responsible for the training of their individual staff in accordance with this Merchant Services Policy document.

IT Contact responsible for setting up e-Commerce/PC Processing (only required for merchants processing online or using credit card processing software)

Name:	
Title:	
Email:	Phone:
Signature:	Date:

IT Security Unit Liaison (SUL) (Required if merchant processing online, using credit card processing software or IP credit card terminals or if required by Treasurer's Office.)
IT SUL Listing: https://www.safecomputing.umich.edu/it-security-professionals/security-unit-liaisons

Name:	
Title:	
Address:	
Signature:	Date:

Department's Budget Administrator - Authority/Approval (required)

Name:	
Title:	
Address:	
Signature:	Date:

To be completed by Treasurer's Office/Merchant Services

Signature:
Date:

Note: Only need to return pages 1, 19 and 21 to the Treasurer's Office via email attachment merchantservices@umich.edu, fax 734 763-2201 or campus mail 10090 Wolverine Tower, 1283.