UNIVERSITY of ROCHESTER

APPROVED BY Ronald J. Paprocki
DATE: 03/03/09; Revised: 11/05/10, 09/10/12; 10/14/14 (MA)
PAGE: 9 total

CREDIT CARD POLICY

I. Policy Statement

Any office of the University that processes credit card transactions may do so only in the manner approved by the University Treasury Office and in compliance with this policy. The Treasury Office requires credit card processing to be done through a single, secure system. This limitation is necessary to secure all Credit Card Information from unauthorized or accidental loss or disclosure and to have uniform compliance with Payment Card Industry (PCI) standards. The University's policy is to comply fully with PCI standards, and with all applicable laws and regulations.

Each office processing credit card transactions must be approved by the Treasury Office as a Merchant, as defined below and must comply with this policy and with the Treasury Office Credit Card Use Requirements, contained in Appendix A.

The Treasury Office has the authority to withdraw or limit Merchant status for failure to comply.

Any office of the University that processes Credit Card Information in violation of this policy and/or the Treasury Office Credit Card Use Requirements may be held financially responsible for any losses, fines, or other costs that the University may incur as a result of fraud, loss of data, or unauthorized access to data or failure to comply with PCI standards or vendor agreements.

Credit Card Information is classified as Legally Restricted under the Information Technology Policy, Section III.D, http://www.rochester.edu/it/policy/documents/INFORMATION_TECHNOLOGY_POLICY.pdf.
Credit Card Information can only be received, held, communicated and disposed of in compliance with the Information Technology Policy, and with the Requirements that are in the Appendix to this policy.

II. Definitions (see also the Glossary in the Appendix)

"Credit Card Information" means a credit card "primary account number" (PAN), which is the 16-digit number on the credit card, the CVV or CVV2 (card security codes), an individual's PIN, the card's expiration date, and the individual cardholder's name.

"Dean" means the highest-level Dean of a school of the University.

"Director" means the Director of the Memorial Art Gallery or of the Laboratory for Laser Energetics.

"Medical Center Finance Officer" means the Associate Director of Financial Services of Strong Memorial Hospital, the Director of Finance and Administration for University of Rochester Medical Faculty Group, the Senior Associate Dean for Finance and Administration at School of Medicine & Dentistry, and the Dean of the School of Nursing.

"Merchant" means a department or other office of the University that is authorized by this policy to accept credit card payments for any services or goods. The term "Merchant" also includes the staff and faculty in the particular department or office.

"PCI Standards" means Payment Card Industry Standards as issued by the Payment Card Industry Security Standards Council, as they may exist from time to time.

"Revenue Receipt FAO and Revenue Category" means a UR Financials revenue ledger account.

"Expense FAO and Spend Category" means a UR Financials spend ledger account.

"Vice President" means a full (i.e., not associate) or Senior Vice President of the University.

III. Merchant Approval.

To be approved as a Merchant, a department or University office must first submit to the Office of Treasury a signed Merchant Agreement, in the form found at the end of this policy and at http://www.rochester.edu/adminfinance/treasury/docs/Credit_card_processing_request.doc
The Merchant Agreement must be signed by the Dean, Director, Medical Center Finance Officer, or Vice President with oversight of the Merchant and by the person under his or her direct or indirect supervision who will be responsible for managing the Merchant's processing of credit cards. By signing the Merchant Agreement, the Merchant and their supervisors are confirming that they have read and agree to comply with this policy and its appendices, and certain other enumerated documents. The Treasury Office will establish a new Merchant account, if it approves the Merchant Agreement.

IV. Responsibilities of Merchants

A. Compliance/Operational.

Each Merchant must:

- Read and comply with this policy, the Requirements in the Appendix to this policy, the Merchant Agreement, and credit card - related documents found at: http://www.rochester.edu/adminfinance/treasury, including "Credit Card Fraud and How to Avoid It," "Guidelines for Card-not-Present Credit Card Transactions," and other similar documents that may be found on the above site from time to time;
- Reconcile daily credit card settlement to revenue received;
- Avoid writing down or encouraging payees from writing down credit card numbers by directing customer to online web site or forward customer to a certified telephone merchant such as Bursar or Gift and Donor Records.
- Attend annual PCI Compliance training session.
- Comply with Address Verification System (AVS) and Card Verification Value (CVV) inclusion for all credit card transactions where cards are non-swiped. Establish and communicate, to its staff and to the Treasury Office, written procedures to limit access to and to protect Credit Card Information as required by this policy;
- Consult the Treasury Office web site regularly for new information;
- Comply with any changes to requirements or processes communicated by the Treasury Office;
- Inform the Treasury Office of any changes to the information provided in the Merchant Agreement;

Changes to an existing Merchant account must be approved by the Treasury Office. Examples of changes include; purchasing, renting, replacing or discarding a terminal, selecting a new virtual service provider, changing an address or telephone number, or closing a location.

No Merchant may enter into any contract, letter of intent, memorandum of understanding, agreement regarding, or make any purchase of, equipment, software, or services, in connection with credit card processing, without the advance written approval of the Treasury Office and either University Information Technology (UIT) or University of Rochester Medical Center's Information Services Division (ISD) (for IT-related purchases and arrangements).

B. Financial. The Merchant will be responsible for paying all costs associated with being a Merchant, including the internal costs of implementation and set-up, the cost of equipment, chargebacks, and ongoing fees to the credit card processor (e.g. Bank of America Merchant Services, American Express, etc.) The Merchant may also be responsible for any fines, fees, costs or liabilities associated with its failure to comply with this policy or with the Merchant agreement.

C. Duties in the Event of Accidental Disclosure or Unauthorized Access. If a Merchant discovers or reasonably suspects that Credit Card Information has been lost, stolen or accessed without authorization, it must immediately report that information to the Treasury Office (treasury@rochester.edu or 585-275-6968) and to UIT or ISD's chief security officer.

D. Audit. The Treasury Office, the Office of University Audit, UIT or the ISD have authority to conduct periodic reviews of Merchant compliance with this Policy and other referenced documents. Each Merchant will cooperate fully in such reviews. Each Merchant will also make its processes, equipments and systems available for access by UIT or ISD and will comply with the requests and direction of those offices as well.

V. Related Policies

Information Technology Policy:
http://www.rochester.edu/it/policy/documents/INFORMATION_TECHNOLOGY_POLICY.pdf

VI. For More Information and Assistance

Contact the Treasury Office at 585-275-6968 or treasury@rochester.edu.

Appendix to Credit Card Policy
The University of Rochester

Treasury Office Credit Card Use Requirements

All UR Merchants must comply with the following in processing credit card transactions. Parenthetical references are to PCI standards. More information is available on the Treasury Office website at http://www.rochester.edu/adminfinance/treasury

A. General Responsibilities for all Merchants

- **Storing electronically the CVV, CVV2 validation code, encrypted PIN block, or PIN numbers is prohibited** – Do not store the three or four digit CVV or CVV2 validation code from the credit card or the PIN, personal identification number (Payment Card Industry (PCI) requirement: **PCI 3.2**).
- **Segregation of duties** – Establish appropriate segregation of duties between the personnel handling credit card processing, the processing of refunds, and the reconciliation function.
- **Mask all but the last 4 digits of the credit card number** – Terminals and software applications must mask or truncate all but the last four digits of the credit card number or if writing down credit card number cannot be avoided, mask immediately after settlement (**PCI 3.3**).
- **Imprint machines are not permitted** – Do not use imprint machines to process credit card payments as they display the full 16 digit credit card number on the customer copy (**PCI 3.4**).
- **Transmitting credit card information by e-mail, instant message, chat, social networking or other electronic means or by fax is prohibited** – Full or partial credit card numbers and three or four digit validation codes (usually on the back of credit cards) may not be faxed or transmitted electronically through such means as e-mail, instant messaging, chat or social networking (**PCI 4.2**).
- **Restrict access based on a business need-to-know** – Access to physical or electronic cardholder data must be restricted to individuals whose job requires access (**PCI 7.1)**.
- **Prevent unauthorized access to cardholder data and secure the data** – Establish procedures to prevent access to cardholder data in physical or electronic form including, but not limited to the following: hard copy or media containing credit card information must be stored in a locked drawer or office; department should establish password protection on computers; visitor sign-in logs, escorts and other means must be used to restrict access to documents, servers, computers and storage media. A registry has been created and will be maintained documenting where all hard copy or media containing credit card information is stored (**PCI 9**).
- **Annual PCI self-assessment questionnaire –** Each location processing credit cards is required to complete an annual PCI self-assessment questionnaire, to be provided by the Treasury Office, for their merchant processing activities.
- **Comply with Information Technology Policy** – Staff must comply with the UR's Information Technology Policy, which addresses physically and electronically safeguarding cardholder information (**PCI 12)**.
- **Document Communication of policies and procedures to staff** – Merchant supervisors must document that they communicated procedures and policies to their staff with operational responsibility. Staff should be asked to sign a document indicating their receipt of the information (**PCI 12.6**).
- **Appropriately label all media** - All media containing credit card information, either electronic or paper copy, must be clearly labeled as "University Confidential - Legally Restricted"
- **Sending/transmission of media should be approved** – Any sending or transmitting of media containing credit card information must be performed by a department administrator level person, and by obtaining approval from Treasury prior to sending/transmitting (**PCI 9.7.1)**.
- **Sending/transmission of media should be in locked mail bags** – Sending and transmitting all media, including daily settlement receipts, should be in locked mail bags with the keys given by department administrator approval only **(PCI 9)**.
- **Anti-virus installation needed** – Any server used in the processing of credit card information must have anti-virus software installed and updated regularly **(PCI 9.6)**.

- **Report Security Incident to the Treasury Office and University IT** – If you know or suspect that credit card information has been exposed, stolen, or misused, report the incident immediately to the following departments:
    1. Treasury Office by e-mail to treasury@rochester.edu.
    2. University IT by e-mail to InfoSecOffice@ur.rochester.edu and by phone to 585-276-3600

       This report must not disclose credit card numbers, three or four digit validation codes, or PINs. The Treasury Office and the University Information Technology departments will then follow the processes outlined in the University's Incident Response document.

B. Responsibilities of University of Rochester Merchants Using a Third Party Service Provider

- The following Merchants are the only ones approved under this policy to use a Service Provider: Memorial Art Gallery (MAG), Strong Memorial Hospital Cafeteria (House of Six Nations), Strong Memorial Hospital Gift Shop, UR Online Card Office, Wilson Commons Student Activities, SMH Specialty Shop, UR Parking, Advancement & Alumni Relations, Graduate Medical Education, and Pharmacy. Anyone seeking a change to a Service Provider or a new Service Provider must consult with the Treasury Office.
- Each of these Merchants must annually submit to the Treasury Office an annual PCI compliance certification provided by the third party service provider.
- These Merchants must comply with the requirements listed above in the "General Responsibilities for all Financial Officers and Systems Managers."
- If the merchant(s) shares cardholder data with service providers, the merchant(s) must comply with the following requirements (**PCI 12.8**):
    - Policies and procedures must be maintained and implemented to manage service providers.
    - Policies and procedures must include a list of service providers, a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess, an established process for engaging service providers, including proper due diligence prior to engagement and a program to monitor service providers PCI DSS compliance status.

C. Training

The Treasury Office will conduct in person or online annual training for Merchants, including:

- PCI compliance
- UR's policies and procedures relating to handling of credit card and other regulated data
- Accepting payment cards
- Merchant account administration
- Consequences for failure to comply with the policy
- Incident response plan
- Security awareness

Merchants (including all staff and application administrators handling credit cards and credit card data) must participate in annual PCI compliance training, provided by Treasury Office.

Online training can be found at http://www.rochester.edu/adminfinance/treasury/

D. Accounting for Transactions

All Merchants will provide a Revenue Receipt FAO including Revenue Category for posting of their credit card receipts. The credit card receipts will be posted electronically to the Revenue Receipt FAO and Revenue Category in UR Financials. Locations will continue to be responsible for daily reconciliation of credit card receipts to daily settlement and revenue generated.

E. Fees

Each credit card transaction is subject to assessment, discount and per item fees charged by Bank of America Merchant Services, Visa, MasterCard, American Express and Discover. All fees, charge backs, fines and penalties will be the responsibility of the Merchant and will be charged to department provided Spend Category.

F. Terminal and Software Security

- All terminals and software must be secured at all times.
- Terminals should be removed to a secure area at the end of each business day if in an open office environment.
- All software on UR systems should be password protected and comply with UR data security policies.
- Appropriate firewalls must be in place to protect access to all credit card data.

G. Disaster recovery

In the event that credit card processing is not operational and you cannot process credit card payments, please comply with the following procedures in the order below. Have your **merchant ID (6749105-xxxx)** and **merchant name** available which is located on the top of the receipt printed from the credit card terminal.

1. Call Bank of America Merchant Services Corp. at **1-800-326-7907** or **1-800-211-2711**. The help desk service representative will be able to assist with diagnosis. Do NOT order any terminal replacements before contacting the Treasury Office.
2. If there is a transmission or communication issue, contact UIT or the ISD support teams for assistance in reconnecting the communication link.
3. If you need a new or replacement terminal or need to update merchant location, call **585-275-3734** to talk with the Treasury Office Financial Accounting Specialist, or e-mail at treasuryoffice@admin.rochester.edu. Guidance will be provided on how to proceed with accepting credit card payments.
4. If none of the above contacts are available, call Assistant Treasurer/Treasury Manager at **585-275-6968** or e-mail at treasury@rochester.edu

H. Supported Terminals

The following are the only credit card devices permitted for use:

FD100
FD200
FD300
FD400 (wireless)
Nurit 3010 (wireless)

Use of any other non-approved device is a violation of this policy and may result in a revocation of merchant processing.

Glossary

Address Verification System (AVS) - The Address Verification Service (AVS)* allows card-not-present transactions to be verified against Visa and MasterCard cardholder's billing address with the card issuer. An AVS request includes the billing address (street address and/or zip or postal). AVS can only be used to confirm addresses in the U.S. and Canada.

CVV Card Verification Value Code (a.k.a. CVV2) – This is a three (3) or four (4) digit number on the back of a credit card.

CISP (Cardholder Information Security Program) – The PCI Data Security Standards were previously issued by Visa and were called CISP.

PABP Software (Payment Application Best Practices) – PABP software is installed on University of Rochester systems and determined by the credit card industry to follow the industry's best practices for securing credit card information. This includes customized, pre-installed, and "off-the-shelf" software and wireless devices. The following link provides a complete list of PCI approved Payment Application vendors. (Note: the list is maintained on Visa's website).
http://usa.visa.com/download/merchants/validated_payment_applications.pdf?it=r|/merchants/risk_management/cisppayment_applications.html

PAN (Primary Account Number) – The 16-digit credit card number.

PED (Pin Entry Device) – Terminal that allows entry of a customer's Personal Identification Number (currently not accepted at UR).

PIN (Personal Identification Number) – Personal number used in debit card transactions (currently not accepted at UR).

Payment Gateway – A payment gateway is a type of service provider that transmits processes, or stores credit card holder data as part of a payment transaction. They facilitate payment transactions such as authorizations and settlement between merchants or processors, also called endpoints. Merchants may send transactions directly to an endpoint or indirectly using a payment gateway. Examples include Paypal/Verisign, Cybersource, and Authorize.net.

Service Provider – A vendor that provides access to the Internet and to applications to facilitate the transfer and/or storage of credit card information.

MERCHANT AGREEMENT UPDATE FOR UR FINANCIALS

For Credit Card Merchant Processing

Complete this merchant agreement for EACH merchant location and send completed document to Office of Treasury, Attn: Kathy King-Griswold, no later than November 1, 2014.
For questions, contact kathy.king-griswold@rochester.edu or 275-6968 or intramural mail to Box 278960.

Operating Manuals for credit card terminals located at: *http://www.rochester.edu/adminfinance/treasury*

……

TO: Kathy King-Griswold, Assistant Treasurer

FROM: _____(Department/Division)

SIGNATURES: _____
(Merchant, Responsible Manager Name and Signature)

_____
(Dean, Director, VP or MC Finance Officer Name and Signature)

Merchant identification number (*begins with 6749105xxx-x*):

I, (Hereafter the "Merchant") agree to accept and process credit card transactions from customers/patients. I have read and will comply with the UR Credit Card Policy, and agree that my school or division will be financially responsible for the cost of implementation, equipment, and set up (approximate cost: virtual $2,000 and dialup $800), ongoing merchant processor fees, daily and monthly reconciliation and any costs or losses incurred due to loss of data or unauthorized disclosure of credit card information processed by my school or division. I agree to require Merchant staff to receive annual training and periodic PCI compliance review. *Merchant will not process any transactions with a manual imprinter.* **If compliance with this agreement is not maintained, credit card acceptance privileges may be revoked.**

If Merchant does not use a credit card terminal and uses software or point of sale software that is PCI approved and approved by the University's PCI project team, the Merchant will provide annual certification of PCI compliance to Office of Treasury.

Depository processing of credit card receipts will be posted to UR Financials automatically. This means that the daily batch settlement processing in your department will automatically post to the RC you provide in this agreement. It is therefore necessary for you to take appropriate actions for special handling of any exceptions that become necessary in the future.

Any changes to data in this agreement must be forwarded to treasury@rochester.edu.

This Merchant location is:

_____Update for UR Financials

_____Replacement terminal if not an FD model, include overnight shipping address, contact name and telephone number (cost is $800 for dial-up and $1,100 for wireless):

_____

Revenue Receipt FAO including revenue category to be charged for the revenue received via credit cards and any chargebacks that occur:

RC | | | | | | | | | | | | | FRS account and sub code_____

Expense FAO including spend category to be charged for the monthly fees, supplies, equipment, etc.:

SC | | | | | | | | | | | | | FRS account and sub code_____

Division department reports to _____(*2 digits, e.g. 50 for SMH*)

Merchant name_____Phone _____

(23 characters maximum, including spaces)

*The merchant name and phone number will appear on the customer's credit card statement. The merchant name is limited to **23** characters, including spaces. It should reflect the department's name in a way that the customer will recognize the charge, e.g. UR Tech Store.*

Processing equipment currently used, include make, model and quantity:

Terminal-dial up _____ **Quantity** _____

Terminal-cellular_____ **Quantity** _____

Virtual Processor (online; include UR ePay#)_____

_____

Physical Address of Department

(*Provide the U.S. Postal address where equipment and documents should be mailed. A name is required on the attention line.*)

Street Address, if available _____

Including Building, Room # _____

City, State, Zip Code _____

Attention _____

Departmental contact _____**Title**: _____

(Person in administrative or managerial position, e.g. Manager, Director, Assistant Director)

Intramural Mail Box # _____Phone _____ Fax _____

Accounting contact _____

(If different from departmental contact) (*Person responsible for creating the daily deposit to record the income collected)*

Intramural Mail Box # _____Phone _____

Chargeback contact _____

(Person responsible for responding to chargeback or dispute information request)

Intramural Mail Box # _____Fax _____