UNIVERSITY OF ROCHESTER

Credit Card Policy

APPROVED BY: Ronald J. Paprocki
DATE: March 3. 2009
PAGE:

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, and no office may have a separate credit card processing arrangement without express approval. This limitation is necessary to help keep all Credit Card Information secure 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.

No office of the University may accept credit cards for payment of any funds due the University unless the office is approved by the Treasury Office as a Merchant, as defined below. Each Merchant 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 accepts or 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, costs or liabilities that the University may incur as a result of fraud, loss of 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. 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 in connection with any of the foregoing.

"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.

"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. The Merchant Agreement indicates that the persons signing it have read and agree to comply with this policy and its appendices, and certain other enumerated documents. If it approves the Merchant Agreement, the Treasury Office will establish a new Merchant account.

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;
- 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);
- Each Merchant must 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
- Merchants must consult the Treasury Office web site regularly for new information;
- Merchants must comply with any changes to requirements or processes communicated by the Treasury Office;
- Merchants must 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 or discarding a terminal, selecting a new service provider, changing an address or telephone number, or closing a location.

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. First Data or Discover). 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 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

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, 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 12 out of the 16 digits of the credit card number** – Terminals and computers must mask or truncate the first 6 digits and the last 4 digits of the credit card number (**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 or fax 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 e-mailed (**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 (**PCI 9**).
- **Annual PCI self-assessment questionnaire –** each location processing credit cards in a not-card-present manner 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. (**PCI12.6**)
- **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.

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.
- 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."

C. Training

The Treasury Office will conduct annual training for Merchants, including:

- PCI compliance and its importance
- UR's policies and procedures relating to handling of credit card and other regulated data.
- Accepting payment cards
- Requesting a merchant ID
- Consequences for failing to follow policy
- Incident response plan

Merchants (including all staff) must participate in the Treasury Office training.

D. Accounting for Transactions

All Merchants must report credit card revenue daily revenue to the appropriate cashiering location and monthly to Finance department.

E. Fees

Each credit card transaction is subject to assessment, discount and per item fees charged by First Data, Visa, MasterCard, American Express and Discover. All fees, chargebacks, fines and penalties will be the responsibility of the Merchant and will be charged to department ledgers.

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. All software on UR systems should be password protected and comply with UR data security policies.

G, Disaster recovery

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

- Call First Data Corp. at **1-800-326-7991**. The help desk service representative will be able to tell you whether the terminal needs to be replaced.
- If you need a new terminal, 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.

- 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 terminal devices allowed for use by Merchants:

Verifone Tranz 380
Verifone Tranz 380x2
Verifone Omni 3750
Verifone vx570
Nurit 8000
Hypercom T7+

Use of any other non-approved device is a violation of this policy and may result in a Merchant losing authorization to process credit card transactions.

Responsibilities for Processing- case examples

Merchant Types	
Credit Card Terminal Merchants Merchants using credit card terminals connected to a data phone line **Requirements** 1. Use terminals that do not print on the customer copy the full 16-digit credit card number. 2. Background checks may be required (PCI 12.7). 3. Secure storage of credit card information. PCI Provisions applicable – PCI 3, 7, 9 & 12	**Internet-related Merchants** **Case A**: Redirecting customers using a link from a UR web page to a PCI approved service provider or to another company's site that is PCI approved. **Case B**: Point of Sale (POS) software that is PCI approved and approved by the University PCI project team. **Case C**: Software that is PCI approved and approved by the University PCI project team. **Case D**: Wireless device and software that is PCI approved and approved by the University PCI project team.

Cases		
	Case A	**Case B**
Description	Redirecting customers to PCI service providers using a link from UR computer. (Merchants do NOT transmit, process, or store credit card data on any computer located on a university IP address.)	Using software that is PABP approved to transmit, process or store credit card information and using PCI approved service providers. (Merchants must submit a request with the Treasury Office.)
Examples	1. UR hosted web page collects all information except credit card information. 2. UR hosted web page is linked to another PCI approved company's site. 3. Paypal/Verisign Payflow Pro.	1. Using point of sale software to transmit, process, or store credit card information. 2. Using a terminal connected to a computer to swipe credit card transactions that are "batched" daily and sent via the Internet. 3. IC Verify, Retail Pro, Shift4
Questions	1. Is service provider PCI approved? 2. Is service provider linked to another service provider? Is yes, is that service provider PCI approved? 3. Does merchant have access to 16-digit credit card numbers? If yes, this is not permitted.	1. Is POS software on the PABP list? 2. Is service provider on the PCI approved list? 3. Is service provider linked to another service provider? Is yes, is that service provider PCI approved? 4. Does merchant have access to 16-digit credit card numbers? If yes, this is not permitted.
Requirements	1. All service providers are PCI approved. 2. Compliance with UR relating to credit cards and information security. 3. No access to 16-digit credit card numbers.	1. Software is on the PABP list. 2. All service providers are PCI approved. 3. Compliance with UR policies relating to credit cards and information security. 4. No access to 16-digit credit card numbers. 5. Background checks may be required (PCI 12.7).
System Requirements	1. Successful external scan. 2. Successful internal scan using University IT approved software. 3. Compliance with university Information Security – Information Handling Guidelines policy. 4. No access or storage of 16-digit credit card numbers.	1. Successful quarterly external scan. 2. Successful periodic internal scan using University IT approved software. 3. Compliance with university Information Security – Information Handling Guidelines policy. 4. No password access or storage of 16-digit credit card numbers. 5. Background checks may be required (PCI 12.7).
	Case C	**Case D**
Description	1. Using software that is PABP approved to transmit, process or store credit card information and using PCI approved service providers.	Using wireless terminals for: 1. Direct transmission of credit card information to a PCI approved service provider. 2. Indirect transmission via a UR server to a PCI approved service provider.
Examples	1. Purchased software & hardware installed on a university computer that transmits to a PCI approved service provider. 2. Software installed by UR on the network. 3. Blackboard, Choice Ticketing, Southern Datacomm	1. Wireless transmission of credit card data using a PAPB approved wireless device. 2. Wireless transmission using a PABP approved wireless device and transmitting via a UR server to a PCI service provider. 3. Nurit 8000
Questions	1. Is software on the PABP list? 2. Is service provider on the PCI approved list? 3. Is the service provider linked to another service	1. Is wireless device and software on the PABP list? 2. Is service provider on the PCI approved list? 3. Is the service provider linked to another service

	provider? Is yes, is that service provider PCI approved? 4. Does merchant have access to 16-digit credit card numbers? If yes, see Financial and System Requirements below.	provider? Is yes, is that service provider PCI approved? 4. If transmitting to a UR server, does merchant have access to 16-digit credit card numbers? If yes, see Financial and System Requirements below.
Requirements	1. Software is on the PABP list. 2. All service providers are PCI approved. 3. Compliance with UR Information Technology Policy and Credit Card Policy. 4. Compliance with Merchant policy regarding access to 16-digit credit card numbers; must be approved in writing by the Treasury Office. 5. Background checks may be required (PCI 12.7).	1. Wireless device and software is on the PABP list. 2. All service providers are PCI approved. 3. Compliance with UR Information Technology Policy and Credit Card Policy. 4. If transmitting to a UR server, merchant policy regarding access and storage of 16-digit credit card numbers approved in writing by the Treasury Office. 5. Background checks may be required (PCI 12.7).
System Requirements	1. Passing systems architecture review by UR PCI project team. 2. Survey successfully completed. 3. Successful quarterly external scan. 4. Successful quarterly internal scan using University IT approved software. 5. Compliance with Information Technology Policy. 6. Compliance with Credit Card policy regarding access to 16-digit credit card numbers and written approval by the Treasury Office. 7. Background checks may be required (PCI 12.7).	1. Passing systems architecture review by UR PCI project team. 2. If transmitting directly to a PCI approved service provider, merchant must comply with Information Technology policy. 3. If transmitting via a UR server to a PCI approved service provider, the following system requirements must be met: a. Survey successfully completed. b. Successful quarterly external scan. c. Successful quarterly internal scan using University IT approved software. d. Compliance with UR Information Technology Policy. e. Compliance with Credit card policy regarding access to 16-digit credit card numbers and written approval by the Treasury Office. f. Background checks may be required (PCI 12.7).

Glossary

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/cisp_payment_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.

UNIVERSITY OF ROCHESTER

MERCHANT AGREEMENT
For Credit Card Merchant Processing

Send the following request to Office of Treasury, Attn: Kathy King-Griswold.
For questions, contact kathy.king-griswold@rochester.edu or 275-6968 or intramural mail to Box 270023.

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

……

TO: Kathy King-Griswold, Assistant Treasurer

FROM: _____

SIGNATURES: _____ (Merchant, Responsible Manager)

_____(Dean, Director, VP or MC Finance Officer

Please approve the issuance of a credit card merchant number to the department of

_____

(Hereafter the "Merchant") 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 of approximately $1,500.00, ongoing merchant processor fees, daily and monthly reconciliation and any costs or losses incurred due to loss 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, then the Merchant will provide annual certification of PCI compliance to Office of Treasury.

This Merchant number is being requested to (**choose one**):

_____ Provide payment for a new product or service, *(explain new product or service):*

_____

_____ Provide another means of payment for an already existing product or service, *(explain existing product or service);*

_____

Estimated Annual Sales Volume _____
(This is the amount you expect to collect per year from the credit card sales.)

Estimated Average Ticket Amount _____
*(This is an estimate of your average ticket price. List only **one** price, not a range, i.e. $10; not $200 to $1,000)*

Expense Account including sub code to be charged for the monthly fees from the merchant processor (s) _____

Authorized Signature for account (*please sign*) _____

Merchant name _____
(23 characters maximum, including spaces)
*The merchant name is the name that will appear on the customer's statement and 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 Computer Sales & Service.*

I will accept the following credit cards types:

MasterCard & Visa _____ (Initials) **Discover** _____ (Initials)

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.*)

Including Building, Room # _____

Street Address, if available _____

City, State, Zip Code _____

Attention _____

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

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 information request)

Intramural Mail Box # _____ Fax # _____