UNIVERSITY of ROCHESTER

APPROVED BY President Richard Feldman
DATE: 12/19/18; Revised: 2/3/16; 1014/14; 09/10/12; 11/05/10
PAGE: 7 total

PAYMENT CARD POLICY

I. Policy Statement

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

Each merchant processing payment 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 Payment 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 or affiliate of the University that processes Payment Card Information in violation of this policy and/or the Treasury Office Payment 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.

Before any new merchant location maintaining Workday/UR Financials may be set up to accept payment card processing, the merchant location will need to have First Notice Rules established. First Notice Rules allow for automatic posting of credits (and debits) in UR Financials, based on the Merchant ID and other identifiers. Further, the merchant would need to agree to have all transactions post to one FAO with the understanding that if additional money movement is necessary from the chosen FAO, the merchant location contact would journal the funds appropriately. If First Notice Rules cannot be established, authorization would need to be obtained by Financial Reporting and Accounting Operations and this authorization provided to the Treasury Office before Treasury would be able to establish a new merchant location and have payment card terminals ordered.

Payment Card Information is classified as Legally Restricted under the Information Technology Policy, Section III.D, http://tech.rochester.edu/policies/information-technology-policy/.
Payment 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)

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

"Dean" or "Director" means the highest-level administrator of a school, division or department of the University.

"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 payment 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.

"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 University Treasury Office a signed Merchant Agreement, in the form located at:
https://www.rochester.edu/adminfinance/treasury/payment-card.html
The Merchant Agreement must be signed by a senior administrator, including 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 payment 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, annual PCI compliance training for staff handling payment cards and/or associated data, and all staff read Payment Card Policy annually. 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 payment card - related documents found at: https://www.rochester.edu/adminfinance/treasury/payment-card.html including "Payment Card Fraud Guidelines" "and other related documents that may be found on the above site from time to time;
- Reconcile daily payment card settlement to revenue received;
- Avoid writing down or encouraging payees from writing down card numbers by directing customer to online web site or forward customer to a certified telephone merchant such as Call Center, Bursar or Gift and Donor Records;
- Complete annual PCI Compliance training session;
- Comply with Address Verification System (AVS) and Card Verification Value (CVV) inclusion for all 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 Payment 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;
- Maintain an inventory of payment terminals or point of sale systems, including make and model of device, location of device (for example, the address of the site or facility where the device is located, device serial number or other method of unique identification), This inventory must be kept current at all times **(PCI 9.9)**;
- Ensure that payment terminals or point of sale systems are periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings **(PCI 9.9)**.

Changes to an existing Merchant account must be approved by the Treasury Office. Examples of

changes include: purchasing, renting, replacing or discarding a terminal or point of sale system, selecting a new virtual service provider, changing an address or telephone number, relocating an office, 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 payment card processing, without the advance written approval of Treasury and Information Security (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 card processor (e.g. Wells Fargo 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 Payment 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 Chief Information Security Officer (abuse@rochester.edu).

D. Audit. The Treasury Office, Information Security and the Office of University Audit 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, equipment and systems available for access by these Offices and will comply with the requests and direction of those offices as well.

V. Related Policies

Information Technology Policy:
http://tech.rochester.edu/policies/information-technology-policy/

VI. For More Information and Assistance

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

Appendix to Payment Card Policy
The University of Rochester

Treasury Office Payment Card Use Requirements

All UR Merchants must comply with the following in processing payment 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 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 card processing, the processing of refunds, and the reconciliation function.
- **Mask all but the last 4 digits of the card number** – Terminals and software applications must mask or truncate all but the last four digits of the card number or if writing down a card number cannot be avoided, mask immediately after settlement (**PCI 3.3**).
- **Imprint machines are not permitted** – Do not use imprint machines to process card payments as they display the full 16 digit card number on the customer copy (**PCI 3.4**).
- **Transmitting card information by e-mail, instant message, chat, social networking or other electronic means or by fax is prohibited** – Full or partial card numbers and three or four digit validation codes (usually on the back of the 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 to cardholder data 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 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 card information is stored (**PCI 9**).
- **Annual PCI self-assessment questionnaire –** Each merchant account owner processing 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 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 card information must be performed by a department administrator level person, and by obtaining approval from Treasury prior to sending/transmitting (**PCI 9.6)**.
- **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 payment card information must have anti-virus software installed and updated regularly **(PCI 5.1)**.
- **Refunds** – Merchants must store all payment card refund PINs securely. If the payment card

password/PIN is noted on the machine itself, payment card privileges may be revoked.

- **Report Security Incident to the Treasury Office and University IT** – If you know or suspect that payment 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 payment 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, Highland Hospital Cafeteria, Strong Memorial Hospital Gift Shop, UR Online Card Office, Wilson Commons Student Activities, UR Parking, Advancement & Alumni Relations, Center for Experiential Learning, Pharmacy, and UR Tech Store. 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

Annual training is required for any individual who has access to payment card data, any data base, end of day balancing, etc. Training is available via the University's MyPath training portal, https://mypath.rochester.edu/ and Net ID. The Treasury Office will conduct in person training for Merchants who may not have access to the MyPath training portal. The training includes:

- PCI compliance
- UR's policies and procedures relating to handling of payment cards 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 payment cards and associated payment card data) must participate in annual PCI compliance training.

Online training can be found at https://mypath.rochester.edu/, entitled, "What is PCI?"

D. Accounting for Transactions

All Merchants will provide a Revenue Receipt FAO including Revenue Category for posting of their payment

card receipts. The payment 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 payment card receipts to daily settlement and revenue generated.

E. Fees

Each card transaction is subject to assessment, discount and per item fees charged by Wells Fargo 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, passwords, and software must be secured at all times.
- All software on UR systems should be password protected and comply with UR Information Security policies.
- Appropriate firewalls must be in place to protect access to all payment card data.

G. Disaster recovery

In the event that payment card processing is not operational and you cannot process payments, please comply with the following procedures in the order below. Have your **Wells Fargo merchant ID (487xxx xxx xxx),** and **merchant name** available which is located on the top of the receipt printed from the processing terminal.

1. A. Call respective bank. The help desk service representative will be able to assist with diagnosis. Do NOT place any order for terminal replacements without contacting Treasury.
   B. Call Wells Fargo Merchant Services Corp. at **1-800-622-0842** for **487xxx xxx xxx** merchant IDs.
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 **585-276-7870** or e-mail at treasury@rochester.edu. . Guidance will be provided on how to proceed with accepting payment card payments.
   If none of the above contacts are available, call Associate Treasurer at **585-275-6968.**

H. Supported Devices

The following are the only devices permitted for use:
FD130 (dial up)
FD410 (cellular dial up)
FD35 (pin pad)
DynaPro/Ingenico 250
iPAD/DynaPad
IDTech, Model: IDSK-534833TEB-B2

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 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 payment card industry to follow the industry's best practices for securing 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 PCI Security Standards website). https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement

PAN (Primary Account Number) – The 16-digit 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 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, Authorize.net and Bluefin.

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