POLICY

Payment Card Policy: Acceptance, Compliance and Governance

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 the Payment Card Industry (PCI) Data Security Standard (DSS). The University must comply fully with the PCI DSS requirements, and all other applicable laws and regulations.

The acceptance of payment cards as a method of payment must only be conducted through a University Merchant account approved by the Treasury Office. All Merchants, as defined below, must comply with both this Payment Card 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 with this Policy and/or any applicable current PCI DSS requirements.

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 due to fraud, loss of data, unauthorized access to data or failure to comply with PCI standards or vendor agreements.

First notice rule must be established for any payment card account.

Payment Card Information is classified as High Risk Information under the Information Technology Policy (https://tech.rochester.edu/policies/information-technology-policy/), Section III.D

Payment Card Information can only be received, held, communicated and disposed of in compliance with the Information Technology Policy (https://tech.rochester.edu/policies/information-technology-policy/), and with the Requirements contained in Appendix A.

II. Annual Policy Review

In compliance with PCI DSS requirements, this policy will be reviewed at least annually and updated as needed to reflect changes to industry standards and/or business objectives and to address new or evolving threats to UR Merchants.

III. Definitions

(see Glossary contained in Appendix A for additional definitions)

“Payment Card Information” means any 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 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 department or office.

“PCI Standards” means Payment Card Industry Data Security Standard as issued by the Payment Card Industry Security Standards Council (PCI SSC).

“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.

IV. 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 for Payment Card Processing found at Payment Card Processing website. (https://www.rochester.edu/adminfinance/treasury/payment-card.html)

The Merchant Agreement must be signed by a senior administrator, including Dean, Director, 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, its appendices, all related policies and certain other enumerated documents, annual PCI compliance training for staff handling payment cards and/or associated data, and that all staff read this Payment Card Policy annually. Upon approval of the Merchant Agreement, a new Merchant account will be established by the Treasury Office.

V. Merchant Responsibilities

A. Compliance/Operational: Responsibilities of each Merchant include but are not limited to the following:

- Read, understand and comply with this policy, the requirements in Appendix A to this policy, the Merchant Agreement, and other payment card related documents and resources found at Payment Card Processing Website (https://www.rochester.edu/adminfinance/treasury/payment-card.html) (documents and other resources provided within the website above are subject to change from time to time);

- Protect Cardholder Data (CHD) and prevent any unauthorized use at all times;

- Reconcile daily payment card settlement reports to revenue received on a regular basis;

- Monitor and address chargeback disputes in a timely manner;

- Writing down payment card numbers and or manually entering cardholder data on behalf of the cardholder is strictly prohibit by the University. Customers must either be directed to an online web site to submit payment or forward to a University approved Call Center, Bursar or Gift and Donor Records Merchant;

- Complete PCI Compliance training session for all staff with payment card processing, reconciliation or data base oversight upon hire and on an annual basis thereafter;

- Comply with Address Verification System (AVS) and Card Verification Value (CVV) fraud controls for all card transactions where cards are non-swiped.

- Establish and communicate written procedures that maintain roles and responsibilities associated with payment card processing to limit access to and to protect Payment Card Information as required by this policy. Procedures must be shared with departmental staff and the Treasury Office;

- Document, with a network diagram, how payment flow occurs within your environment.

- Consult the Treasury Office web site (https://www.rochester.edu/adminfinance/treasury/payment-card.html) 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 current list of all MIDs that includes Merchant location and authorized users;
- Maintain an inventory of payment terminals and/or point of sale systems that include the make and model of device, device serial number or other method of unique identification, location of device (for example, the address of the site or facility where the device is located).), This inventory must be kept current at all times;
- 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.
- For those using payment gateways, work with your technical support staff to ensure that all payment page scripts that are loaded and executed in the consumer's browser are managed as follows:
    - A method is implemented to confirm that each script is authorized.
    - A method is implemented to assure the integrity of each script.
    - An inventory of all scripts is maintained with written justification as to why each is necessary.

Changes to an existing Merchant account must be approved by the Treasury Office. Examples of a change include, but not limited to: purchasing, renting, replacing or discarding a terminal or point of sale system, selecting a new service provider, a change in main contact responsible for the account, 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).

Data Retention/Storage: Electronic storage of Primary Account Number (PAN) and/or Sensitive Authentication Data (SAD) even if encrypted is prohibited, refer to the following University policies:

- Data Security Classification Policy (https://www.rochester.edu/policies/policy/data-security-classifications/)
- Information Technology Policy (https://tech.rochester.edu/policies/information-technology-policy/)

B. Financial: The Merchant is 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 all other ongoing processing fees to the payment card processor (e.g., Wells Fargo Merchant Services, American Express, JPMorgan Paymentech,) 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.

Prior to accepting payment cards as a method of payment, any potential Merchant that utilizes workday/UR Financials, must establish First Notice Rules. 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 must 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 must manually journal the funds appropriately. If First Notice Rules cannot be established, authorization must be obtained by Financial Reporting and Accounting Operations and provided to the Treasury Office before a new Merchant location is established by Treasury.

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 (mailto:treasury@rochester.edu) or 585-275-6968) and to the University Information Security Team (abuse@rochester.edu (mailto: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 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.

VI. Related Policies

Information Technology Policies:

- Information Technology Policy (https://tech.rochester.edu/policies/information-technology-policy/)
- IT Policies (https://tech.rochester.edu/policy/)

VII. For more information and assistance

Contact the Treasury Office at 585-275-6968 or via email to merchant_support@ur.rochester.edu (mailto:merchant_support@ur.rochester.edu) or treasury@rochester.edu. (mailto:treasury@rochester.edu)

Appendix A

Treasury Office Payment Card Use Requirements

All UR Merchants must comply with the following in processing payment card transactions. More information is available on the Treasury Office website (https://www.rochester.edu/adminfinance/treasury/payment-card.html)

A. General Responsibilities for all Merchants (according to the latest version of the PCI DSS)

- **Storing the CVV, CVV2 validation code, encrypted PIN block, or PIN numbers is strictly prohibited** – Do not store the three or four digit CVV or CVV2 validation code from the card or the PIN, personal identification number.

- **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.

- **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.

- **Transmitting card information by e-mail, instant message, chat, social networking or other electronic means or by fax is strictly 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.

- **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.

- **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 A registry has been created and will be maintained documenting where all hard copy or media containing card information is stored.

- **Annual PCI Assessments** – Each merchant account owner processing payment cards must work with and answer all communications from the Treasury Office and associated parties in a timely manner, for their merchant processing activities.

- **Comply with Information Technology Policy** – Staff must comply with the UR's Information Technology Policy (https://tech.rochester.edu/policies/information-technology-policy/), which addresses physically and electronically safeguarding cardholder information.

- **Document Communication of policies and procedures to staff** – Merchant supervisors must document that they communicated procedures and policies to their staff with operational Staff should be asked to sign a document indicating their receipt of the information.

- **Electronical sending or transmitting cardholder data is strictly prohibited.** – This includes but is not limited to, sending data via email, text messaging and social media.

- **Physical transport of any form containing cardholder data must be transported in locked mail bags** – This includes but is not limited to daily settlement receipts, mail order forms and access to locked mail bags must be given by department administrator approval only.

- **Anti-virus installation needed** – Any server used in the processing of payment card information must have anti-virus software installed and updated regularly.

- **Passwords/PINs** – Merchants must store all device PINs and passwords securely and must never be noted on the device itself or in public view. Failure to comply with this requirement may result in payment card privileges being revoked.

B. Responsibilities of Merchants Using a Third Party Service Provider

- Explicit approval from the Treasury Office is required to use any Third Party Service Provider (TPSP).. Any changes from an existing TPSP and/or requests to contract with a new TPSP must be presented to and approved by the Treasury Office.

- All Merchants utilizing TPSPs must obtain updated documentation from the TPSP illustrating their PCI compliance and submit the documentation to the Treasury Office on an annual basis.

- 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 all applicable requirements contained within the latest version of the PCI DSS, including but not limited to the following:

    - Policies and procedures must be maintained and implemented to manage service

    - 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

Any individual with access to payment card data and/or any related database, systems, software, end of day balancing, etc. is required to complete PCI Compliance Training upon hire and on an annual basis thereafter. The training is available via the University's MyPath training portal (https://mypath.rochester.edu), entitled, "What is PCI?" 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 this policy
- Incident response plan
- Security awareness
- Device inventory monitoring and list

D. Accounting for Transactions

All Merchants must provide a Revenue Receipt FAO including Revenue Category for posting of their payment card receipts to General Accounting. The payment card receipts will be posted electronically to the Revenue Receipt FAO and Revenue Category in UR Financials. All Merchants must reconcile all payment card receipts to revenue generated on a daily basis.

E. Fees

Each card transaction is subject to assessment, discount and per item fees charged by the University's payment card processor (s), as well as Interchange fees charged by 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 provided Spend Category.

F. Terminal and Software Security

- All terminals, passwords, and software must be always secured.
- All software on UR systems should be password protected and comply with UR Information Security
- All individuals with approved access should have their own unique username and password.
- Group/shared usernames and passwords are strictly prohibited.
- Appropriate firewalls must be in place to protect access to all payment card

G. Troubleshooting

In the event payment card processing is not operational, and payments cannot be processed, email merchant_support@ur.rochester.edu (mailto:merchant_support@ur.rochester.edu) or call 585-276- 7870 for assistance. If known, provide your merchant ID (487xxx xxx xxx), and/or merchant name and provide details of the issue you are experiencing.

H. Supported Devices

Only devices approved by the UR Treasury Office are permitted for use. All devices used for payment processing must be ordered through the UR Treasury Office

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

Incident Response Plan

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:

- Treasury Office by e-mail to treasury@rochester.edu (mailto:treasury@rochester.edu).
- University IT Help Desk: univithelp@rochester.edu (mailto:univithelp@rochester.edu) and (585) 275-2000

Never disclose payment card numbers, three or four digit validation codes, or PINs. The Treasury Office and the University Information Technology departments will follow the processes outlined in the University’s Incident Response document.

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 is only used to confirm addresses in the U.S. and Canada.

- **Card Brands –** American Express, Discover, JCB, MasterCard or Visa.

- **Cardholder Data (CHD) –** At minimum, consists of the full PAN but may also include the full PAN with cardholder name, expiration date, or service code.

- **Cardholder Data Environment (CDE)** – The people, processes and technology that capture, store, process or transmit CHD or SAD, including any system components that may affect the security of such data.

- **Chargeback** – A charge that is returned to a payment card and debited from the Merchant after a customer disputes an item on their account statement.

- **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.

- **Merchant ID (MID)** – Unique ID associated with each UR Merchant account used for transaction processing and billing.

- **Third Party Service Provider (TPSP) –** Any business entity that is not a Card Brand and is directly involved in the processing storage or transmission of CHD, or that provides services that control or could impact the security of the CDE.

- **PAN (Primary Account Number)** – Also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the cardholder account and consists of 16 to 19 digits.

- **PCI SSC** – Payment Card Industry Security Standards Council made up of five Card Brand members that set the standards to enhance CHD security.
- **PCI DSS** – Payment Card Industry Data Security Standard – provides a baseline of technical and operational requirements designed to protect CHD which applies to all entities that store, process or transmit CHD or SAD and/or are involved in credit card processing.
- **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.
- **SAD** – Sensitive Authentication Data – Security related information used to authenticate cardholders and/or authorize credit card transactions, includes full track data, equivalent data on the chip, three- or four-digit code (e.g., CVV2), or Personal identification number (PIN) entered by cardholder during a card present transaction, and/or encrypted PIN block present within the transaction message.
- **Service Provider** – Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the

security of cardholder data. Examples include managed service providers that provide managed firewalls, intrusion detection systems and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

Appendix B

Documentation supporting data flow is a requirement of PCI DSS. The PCI Security Standards Council (PCI SSC) has created interactive tools to help identify and document your current environment. Review the guide (HTTPS://WWW.ROCHESTER.EDU/POLICIES/WP-CONTENT/UPLOADS/2024/10/PAYMENT-CARD-POLICY-APPENDIX-B.PDF)

ABOUT THIS POLICY

Policy Applies To

Staff

Issuing Authority

Administration & Finance

<iframe src="https://www.googletagmanager.com/ns.html?id=GTM-TT7PP8Z" height="0" width="0" style="display: none; visibility: hidden" ></iframe >