PCI-DSS Compliance (Payment Card Industry Data Security Standards)

ROWAN UNIVERSITY POLICY

Title: *PCI-DSS Compliance (Payment Card Industry Data Security Standards)*
Subject: *Credit and Debit Card Payments*
Policy No: *Fin: 2019:01*
Applies: *University-Wide*
Issuing Authority: *President*
Responsible Officer: *Senior Vice President for Finance & CFO; Senior Vice President for Information Resources and Technology & CIO*
Adopted: *03/18/2019*
Last Revision: *03/07/2023*
Last Reviewed: *03/07/2023*

I. PURPOSE

The purpose of this policy is to:

a. Establish University-wide standards to ensure PCI-DSS compliance.
b. Provide guidance to individuals with responsibility, authority, and stewardship over credit card and debit card payments.
c. Minimize institutional risks associated with data breaches resulting from PCI-DSS non-compliance.

II. ACCOUNTABILITY

At the direction of the Senior Vice President for Finance & CFO (SVP & CFO) and the Senior Vice President for Information Resources and Technology & CIO (SVP & CIO), the University's PCI Compliance Committee shall implement and maintain this policy. The Vice Presidents, Deans, and other members of management shall implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all individuals who have the responsibility, authority, and stewardship over credit card and debit card payments processed by the University, and those who process credit and debit card payments on behalf of the University.

IV. DEFINITIONS

1. **Payment Card Industry Data Security Standards (PCI-DSS):** PCI-DSS are a set of security standards designed by the PCI Security Standards Council to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment to protect and safeguard cardholder personal information and data.
2. **PCI Security Standards Council:** An organization created by the major credit card companies in an effort to better protect credit card data.
3. **Attestation of Compliance (AOC):** This document must be completed by a Qualified Security Assessor (QSA) or by the merchant as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard.

4. **Qualified Security Assessor (QSA):** A designation conferred by the PCI Security Standards Council to those individuals that meet specific information security education requirements, have taken the appropriate training from the PCI Security Standards Council, are employees of a Qualified Security Assessor (QSA) company or approved PCI security and auditing firm, and will be performing PCI compliance assessments as they relate to the protection of credit card data.
5. **Self-Assessment Questionnaire (SAQ):** The SAQ is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the Payment Card Industry Data Security Standard. This questionnaire is filled out on a yearly basis by the PCI Compliance Committee. The SVP & CFO is the officer responsible for signing the attestation of compliance.
6. **Approved Scanning Vendor** (**ASV):** This is a third party organization that is certified to perform external IP address network vulnerability scans that are done to ensure all PCI compliance requirements are met.
7. **Merchant:** An area or department of the University that accepts payments by way of credit or debit card for goods, services, and other University related items. Each department is issued a Merchant ID by Rowan's Approved and Exclusive Third Party Credit Card Processor.
8. **Cardholder Data (CHD):** Any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder data includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date or service code.
9. **Sensitive Authentication Data (SAD):** Security-related information including, but not limited to, card validation codes/values (e.g., three-digit or four-digit value printed on the front or back of a payment card, such as CVV2 and CVC2 data, full magnetic stripe data, PINs, and PIN blocks used to authenticate cardholders and/or authorize payment card transactions.
10. **Virtual Credit Card:** A temporary credit card number that typically can only be processed one time for an exact dollar amount.
11. **Card Skimmer:** A device that is attached to a credit card reader or it's wiring and is used to collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder.

    Refer to the Rowan University Technology Terms and Definitions for technology terms and definitions that are used in this policy.

V. POLICY

1. PCI Compliance Committee

    a. The University shall establish and maintain a PCI Compliance Committee to manage and oversee compliance with the PCI Standards set forth by the Payment Card Industry Security Standards Council.
    b. The Office of the Bursar and the Information Security Office shall designate members to the PCI Compliance Committee.
    c. The Office of the Bursar and the Information Security Office shall have equal decision making authority within the PCI Compliance Committee.
    d. The PCI Compliance Committee must maintain an inventory of all approved payment processing systems and merchant equipment to ensure only PCI-compliant hardware and software is in use.
    e. The PCI Compliance Committee must review all AOCs on an annual basis.
    f. The PCI Compliance Committee must complete the required SAQs on an annual basis for each credit card processing merchant.
    g. The PCI Compliance Committee must ensure regularly scheduled network scans (if applicable) are completed by an approved scanning vendor.
    h. The PCI Committee will notify any merchant found to be out of compliance and ensure appropriate mitigation plans are developed and implemented to bring them into compliance.
    i. This committee will provide training on PCI compliance procedures as needed and/or upon request.
2. Merchant Registration:
    a. New Registration

        i. Departments looking to process credit card transactions on behalf of the University for the first time must submit a Rowan University Credit Card Processing Merchant Request Form to be considered for approval by the PCI Compliance Committee.
    b. Existing Registration
        i. Departments already processing credit card transactions that are interested in changing their existing processing environment must also submit a Rowan University Credit Card Processing Merchant Request Form to be considered for approval by the PCI Compliance Committee.
    c. All credit card processing systems must be compatible with the University's Approved and Exclusive Third Party Credit Card Processor.
    d. New merchant requests require a new merchant contract to be established between Rowan's Approved and Exclusive Third Party Credit Card Processor and Rowan University. CFO or the CFO designee signature is required.
    e. All software and equipment that is connected to a new or existing merchant must be approved prior to implementation.
    f. Requestors are responsible for all costs associated with credit card processing software and equipment.
3. Credit Card Readers and Online Payment Gateways:
    a. All payment processing systems and services must be reviewed and approved through the ITAP process and the PCI Compliance Committee prior to use at the University.
    b. All credit card readers must be listed as approved devices on the PCI Security Standards Council website.
    c. All credit card readers must be configured with Point to Point Encryption Solutions that are listed on the PCI Security Standards Council website.
    d. All secure online Payment Gateway technology must have a valid and up to date PCI-DSS Attestation of Compliance (AOC). The AOC must be issued within the last year and reviewed on an annual basis.
    e. Non-mobile credit card processing devices and systems (such as DESK3500 and ipp320 with Bill and Pay) must be connected directly (hard wired) to the secure Rowan University network.
    f. Mobile or wireless credit card processing devices must communicate by way of a cellular connection and cannot connect over wifi.
4. Merchant Compliance:
    a. All University merchants must maintain compliance with this policy and related procedures.
    b. Merchants that are out of compliance with this policy must work with the PCI Compliance Committee to address and resolve any deficiencies immediately.
    c. Merchants unable to maintain PCI Compliance will have their ability to accept credit cards suspended or revoked.
5. Processing Cardholder Data:
    a. Cardholder data can only be received in-person to be processed through a credit card reader, online through a secure payment gateway or by way of postal mail in which case it is also processed through a credit card reader.
    b. Cardholder data cannot be received or exchanged over the telephone.
    c. Cardholder data cannot be emailed, faxed, scanned or printed.
        i. Receipts generated by credit card readers and online payment gateways with properly truncated credit card numbers are acceptable.
    d. If cardholder data is received by email or fax, notify the sender that the payment cannot be processed. Notification cannot contain credit card information. Ensure original email with credit card information is deleted.
    e. Personal devices such as computers, laptops, phones and other end user devices may not be used to exchange or process credit card data.
    f. Offices receiving cardholder data via postal service must maintain:
        i. A locked mailbox for delivery of incoming mail.
        ii. A locked safe for in-process storage.
    g. If not being processed immediately, mail with card holder data must be stored in the locked safe. Credit card data should never be left unattended.
    h. Credit card data captured on mailed in paper forms must be redacted using redacting pens, and then shredded immediately after processing.

i. Forms used to capture credit card data must be approved by the PCI Compliance Committee.
ii. Forms used to capture credit card data cannot include e-mail addresses and fax numbers.

i. Rowan University staff, departments and its systems do NOT retain any credit card data. The retention period for credit card data at the University is zero days.
j. Staff members processing credit card data should each have their own log in to both the RU network and credit card processing software being used. IDs and passwords should not be shared.
k. Credit card data cannot be entered via a computer keyboard or other non-approved data entry devices.
l. Please contact the PCI Compliance Committee, through the Office of the Bursar, if you have questions about how to process credit card not present refunds. SOM Medicine Offices should contact the Central Billing Office about credit card not present refunds.
m. Although virtual credit card numbers do not fall within the scope of PCI compliance, if a department anticipates receiving virtual credit card data they should inform the PCI Compliance Committee.

6. Credit Card Reader Maintenance:
   a. Department supervisors are responsible for ensuring all credit card reader devices used within their department are inspected at the start of each business day.
      i. Verify that non-mobile devices are fully hardwired to the Rowan University network. Processing with non-mobile devices wirelessly through laptops is prohibited.
      ii. Look for signs of tampering.
      iii. Verify that card skimmers have not been added to the device.
      iv. Verify the device has not been replaced with a different device.
   b. Department supervisors must implement the Credit Card Reader Daily Inspection Log that will track the daily inspection of credit card readers. These logs must be kept in a safe location for a period of two years.
   c. Only Rowan University employees should inspect credit card reader devices.
   d. All credit card reader devices must be safeguarded and out of public reach.
   e. If a credit card reader device is no longer needed it needs to be returned to the PCI Compliance Committee. Please notify the Office of the Bursar if necessary.
   f. Credit card reader devices cannot be transferred or relocated without approval from the Office of the Bursar.
7. Additional Merchant Responsibilities:
   a. It is the responsibility of the supervisor overseeing a department that is processing credit card or debit card payments to ensure they work with the PCI Compliance Committee to:
      i. Ensure that all employees processing or with access to cardholder data are properly trained via the review of this document, the completion of Rowan University's PCI Compliance Training and any other required security training set forth by IRT.
      ii. Identify positions that require access to payment card data and system components and limit access to only employees whose jobs' require such access. Be sure to deactivate /remove access when they no longer require access to cardholder environments.
         1. This may require contacting the Office of the Bursar.
      iii. Provide a proper control environment, including segregation of duties, for processing payment card transactions.
   b. Department managers are responsible for overseeing the processing of refunds.
   c. Only department managers or designated staff should have access to process credit card refunds.
   d. If a credit card reader or system allows for a passcode to be entered in order to process a refund the manager should have the refund passcode set-up and ensure that it is distributed to only limited designated staff that are allowed to process refunds.
   e. It is the responsibility of all Rowan University personnel to notify the PCI Compliance Committee (Office of the Bursar and Information Security Office) immediately in the event of suspected fraud or data breach.
      https://confluence.rowan.edu/display/POLICY/Security+Incident+Management+Policy