RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Payment Card Acceptance Policy				
Section #:	40.2.15	**Section Title:**	Financial Management: Fiscal Management	**Formerly Book:**	N/A
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer	**Adopted:**	01/25/2010	**Reviewed:**	06/07/2021
Responsible Executive:	Associate Vice President and Associate Treasurer	**Revised:**	07/01/2013; 10/10/2013; 06/07/2021 (complete rewrite)		
Responsible Office:	University Treasury	**Contact:**	University Treasury: 848-445-3353 treasury@finance.rutgers.edu		

1. **Policy Statement**

   Rutgers University requires that any individual who is involved in the collection of card payments must adhere to the University's information technology security practices, specific requirements related to payment card transactions, as well as the required best practices prescribed by the Payment Card Industry Data Security Standards (PCI-DSS or PCI Compliance).

2. **Reason for Policy**

   To provide the University community with clear and manageable guidelines to protect sensitive customer data including cardholder data, which in turn protects the University's reputation, reduces the risk of fines, and enables the University to continue the practice of accepting card payments.

3. **Who Should Read This Policy**

   Any individual who handles, processes, supports, stores, disposes of, or otherwise manages payment card transactions or information on behalf of the University.

4. **Resources**

   - University Treasury Credit Card Acceptance website
   - IT Risk, Policy, and Compliance training website
   - PCI Security Standards Council website
   - University Policy 30.4.5: Records Management
   - University Policy 70.1.1: Acceptable Use Policy for Information Technology Resources
   - University Policy 70.1.3: Incident Management Policy
   - Incident Reporting Information

5. **Definitions**

   Card Verification Value (CVV2 or CVV) - A three-digit number on the back or four-digit number on the front of a payment card. PCI does not permit the CVV2/CVV to be stored on paper, electronically, or by any other means.

Cardholder Data - Any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side.

Merchant – University department that accepts card payments.

Merchant ID – The identification number assigned to each merchant by the credit card processor that acts as a unique identifier for that payment process.

P2PE – Point to Point Encryption – PCI-DSS verified software that cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.

Payment Card – Credit and debit cards issued by a card brand such as Visa, MasterCard, American Express, and Discover.

PCI-DSS - A mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment.

PCI Steering Committee – University committee charged with establishing security requirements for University merchants.

Self-Assessment Questionnaire (SAQ)– Form that is required to be filled out annually by every merchant attesting that the systems and procedures related to card processing are compliant with PCI-DSS.

6. **The Policy**

A. New Merchant Requests

a. Requests for new Merchant ID's must be routed to University Treasury for review and approval.
b. All new card processing setups, vendors, systems, etc. must be reviewed and approved by Office of Information Technology (OIT) Information Protection and Security.
c. Departments should use a payment processing vendor that has been previously reviewed and placed on the approved vendor list, unless granted an exception by University Treasury.
    i. All new payment collection processes must be reviewed by OIT Security even if the vendor is on the approved list, as there could be differences in setup and/or process.
d. All new merchants must provide the following details to University Treasury:
    i. Department name
    ii. Merchant ID(s)
    iii. Merchant contact person/people who will be responsible for completing the annual SAQ form(s)
    iv. General Ledger (G/L) accounting strings for fees and revenues for the automation of accounting, where possible

B. Security Objectives

a. Minimizing Risk:
    i. New and existing merchants should consider ways to reduce the risk of compromising cardholder data through loss or theft such as utilizing encryption of cardholder data, tightening departmental processes and controls, outsourcing the merchant ID and/or payment transactions to a PCI-validated third party, etc.
b. Ensuring Compliance with PCI-DSS:

MERCHANT COMPLIANCE GOALS	PCI-DSS REQUIREMENTS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software and programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

C. Merchant Responsibilities

a. Security of the environment
   i. Secure access, storage, and handling of credit card machines
   ii. Adequate security of the network environment, as determined in consultation with OIT
b. Complete the relevant SAQ form(s) on an annual basis for each merchant
c. Annual online training through OIT-IT Risk, Policy, and Compliance for any and all individuals involved in the processing of payment card transactions
d. Documentation
   i. Inventory of all devices, workstations, laptops used for inputting cardholder data
      1. Make/Model
      2. Serial Number
      3. Description of Use/Purpose
   ii. Inspection logs of all payment card processing equipment
   iii. Inventory of all software/websites/applications used for payment card acceptance
   iv. Payment card handling / Authorization Data Flow Diagram
   v. Departmental payment card procedures
      1. Payment processing procedures
      2. Procedures for physical security of the devices
      3. Incident response procedure
   vi. Listing of all staff involved with accepting or handling credit cards, including a description of their role (e.g., cashier, approver)

D. Minimum Security Requirements

a. Network-Connected Devices:
   i. Any payment collection devices (card readers, POS systems, kiosks, etc.) that utilize the University's network to transmit cardholder data must utilize PCI-certified point-to-point encryption (P2PE) when processing transactions.
      1. This does not include "outsourced" payment transactions that only use the University's network to redirect to a payment site hosted by a third party (e.g., PayPal).
b. Storage, Retention, and Destruction of Cardholder Data:
   i. Cardholder Data should *never* be stored electronically without encryption or transmitted or accepted via email.

ii. Cardholder Data that is written on a piece of paper should not be stored and must be disposed of promptly through cross-cut shredding, incineration, or through an approved secure shredding and disposal service through Institution Planning & Operations.

c. Payment Devices:
   i. Card readers, POS terminals, etc. should be inspected regularly, at least quarterly – more often depending on the environment, to identify possible tampering.
      1. An inspection log should be kept that documents who inspected the machine.
   ii. Card readers should not be left unattended and should be securely locked away when not in use.

d. Potential Breach Response:
   i. If a breach of cardholder data is suspected, the department must contact abuse@rutgers.edu immediately and follow the department's incident response plan (see https://it.rutgers.edu/knowledgebase/reporting-suspected-scams-breaches-or-theft/).

e. Vulnerability Scanning
   i. Any devices or systems that transmit payment card data to the public internet must be scanned on a quarterly basis by an approved PCI scanning vendor, coordinated by University Treasury.
      1. IP addresses of such devices and any updates or changes to those IP addresses must be provided to University Treasury prior to changes being implemented in production.

E. Failure to Comply

a. Failure of merchants to comply with any of the security and compliance requirements outlined in this policy, such as completion of annual training or the annual SAQ, or requirements otherwise assigned by University Treasury and/or OIT, can result in the termination of that merchant's ability to collect card payments.