RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

**RUTGERS POLICY**

**Section:** 40.2.15

**Section Title:** Fiscal Management

**Policy Name:** Payment Card Acceptance Policy

**Formerly Book:** N/A

**Approval Authority:** Senior Vice President for Finance and Treasurer

**Responsible Executive:** Senior Vice President for Finance and Treasurer

**Responsible Offices:** Office of Treasury Operations and Office of Information Protection and Security

**Originally Issued:** 01/25/2010

**Revisions:** 7/1/2013, 10/10/2013 (Updated title)

**Errors or Changes**: **Contact**: Office of Treasury Operations at 848-445-3787

1. **Policy Statement**
   It is the position of the university to provide safeguards to protect information and data in accordance with federal, state and industry requirements. Therefore, any department that accepts, processes, stores and transmits payment card data must be in compliance with the Payment Card Industry Data Security Standards. The security standard applies to all types of payment card transactions including in-person, mail, telephone and web transactions. This document provides the policy framework through which departments must implement data protection standards in order to ensure compliance. This policy applies to all Rutgers University departments, faculty, staff, students, organizations and individuals who, on behalf of the University, handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all Rutgers University locations, whether on or off campus.

2. **Reason for Policy**
   - To ensure that all individuals in departments that accept confidential payment cards as a form of payment for university goods and services understand their responsibility to protect the data in accordance with the Payment Card Industry Data Security Standards and subsequent revisions to the standards.
   - To ensure that all external organizations contracted by University departments, faculty, staff, students, organizations and individuals to provide outsourced services for credit or debit card processing for University business understand their responsibilities to protect the data.

3. **Who Should Read This Policy**

All members of the Rutgers University community

University administrators including, but not limited to:

- Chancellors and vice presidents
- Deans, directors, chairs, and department heads
- Administrators, managers, supervisors

All third party vendors / service providers who collect, process or store payment card data on behalf of the university.

4. **Related Documents**

a. Rutgers Gramm-Leach-Bliley Act (GLBA) Information Security Policy 50.3.11
http://policies.rutgers.edu/PDF/Section50/50.3.11-current.pdf

b. Rutgers Identity Theft Compliance Policy 50.3.9
http://policies.rutgers.edu/PDF/Section50/50.3.9-current.pdf

c. Payment Card Industry Data Security Standard (PCI-DSS)
https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

d. Visa Cardholder Information Security Program
http://usa.visa.com/business/merchants/cisp_index.html

e. DRAFT Rutgers Information Security Classification Policy
http://rusecure.rutgers.edu/drupal/?q=content/draft-information-security-classification-policy

f. Rutgers Internet Technology Security Standards
http://rusecure.rutgers.edu/

g. Rutgers Credit Card Protection Security Standards
http://treasury.rutgers.edu/payment-card-acceptance/creditdebit-card-security-policies

h. Contract Addendum Concerning Protected Information
https://purchasing.rutgers.edu/

5. **Contacts**

a. Rutgers Information Protection and Security
https://rusecure.rutgers.edu/contact

b. Vice President for Finance and Associate Treasurer
848-445-3787
TO@treasury.rutgers.edu

6. **The Policy**

## 40.2.15 PAYMENT CARD ACCEPTANCE POLICY

I. **Policy Details**

All transactions (including electronic based) that involve the transfer of payment card information must be performed on the systems approved by the university's Vice President for Finance and Associate Treasurer (Vice President), after a prior security review by the Director of Information Protection and Security (Director). All applications that have been approved for payment card activity must be administered in accordance

with the requirements of all Rutgers University policies and the Payment Card Industry Data Security Standard (PCI-DSS).

The Vice President will be responsible for monitoring and communicating to the university community any changes that are made to the PCI-DSS and industry best practices as they relate to acceptance of payment card payments through card swipe terminals. The Director will monitor and communicate changes to the PCI-DSS and industry best practices as they relate to acceptance of credit card payments through e-commerce.

Departments that need to accept payment cards and obtain a physical terminal to either swipe or key transactions through the point of sale terminals must contact the Vice President to obtain approval and a Merchant Number and to receive training and instructions on how to record those transactions and reconcile their accounts on the university's accounting system.

Departments that need to engage in electronic commerce are required to use the methodology approved by the Vice President for Finance and Associate Treasurer and are required to work with The Office of Information Protection and Security to ensure the e-commerce application meets all university policies, recommended security standards, and the PCI-DSS.

## II. Credit Card Security Standard Procedures

It is the policy of the university that all staff, faculty and students that accept credit or debit cards in the normal pursuit of business for their department or student organization do so in a secure manner as set forth by the PCI-DS. It is the responsibility of the staff, faculty, and students to ensure all sensitive cardholder data are protected against fraud, unauthorized use or other compromise.

Please refer to the security standards and "Related Documents" listed under item 4 for additional information. Please refer to the Cash Handling Policy and Procedures memo distributed by the Office of Treasury Operations for best practice procedures that should be follow to aid in the compliance with this policy.

## III. Protection Standards

The Rutgers Security Standards have been developed in order to provide direction on appropriate system, administrative, and physical controls (based on sensitivity) that should be applied to data. Therefore, University data will be protected by implementing one of the standards below based upon the data classification.

1. Rutgers Security Standard for Protecting Restricted Data
   http://rusecure.rutgers.edu/content/glba-security-standards

2. Rutgers Security Standard for Protecting Networked Devices
   https://rusecure.rutgers.edu/category/topic/minimum-security-standards-networked-devices

## IV. External Consequences

Failure to meet the requirements outlined in this policy may result in suspension by the Payment Card Industry (Visa, MasterCard, Discover, American Express, etc.) of the Business Unit's and / or the University's privilege of accepting payment cards. Additionally, should sensitive card holder data be compromised as a result of the failure to meet the requirements of the PCI DSS, fines may be imposed on the University by the Payment Card Industry, beginning at $50,000 for the first violation. Departments will be expected to absorb these fines along with all costs or penalties / fees assessed as a

result of security violations including, but not limited to, costs necessary to notify customers that their confidential information has been compromised.

Some violations of the PCI DSS may constitute criminal offenses under local, state, and federal laws. The university will carry out its responsibility to report such violations to the appropriate authorities.

## V. Internal Consequences

Failure to meet the requirements outlined in this policy will result in Treasury Operations deactivating the merchant identification number, thereby suspending payment card acceptance for the affected business units. Merchant identification numbers will be reactivated only when the affected business unit is once again compliant with this policy.

Persons in violation of this policy are subject to the full range of sanctions, including, but not limited to, the loss of computer or network access privileges, disciplinary action, suspension, termination of employment, dismissal from the university, and legal action.