New Jersey Institute of Technology **Effective Date:** October 31, 2024
University Policies

Sponsoring Functional Area: Financial Systems & Innovation (FSI)

Subject/Title: Department Credit/Debit Card Acceptance Policy

I. Policy Statement

The University accepts credit/debit cards for goods and services, adhering to applicable laws and Payment Card Industry Security Standards Council (PCI SSC) regulations. The protection of cardholder data is a fiduciary responsibility shared by the University and its merchants. The University has partnered with several Merchant Service Providers (MSPs) to provide integrated, comprehensive, and secure commerce and credentials solutions for processing credit/debit card payments. This policy outlines the standards, procedures, and responsibilities for handling credit/debit card transactions to safeguard sensitive cardholder data.

II. Purpose

The purpose of this policy is to establish and define responsibilities, guidelines and best practices for University entities engaging in the acceptance, processing, and transmitting of credit/debit card payment data and to ensure proper control, integrity, and protection of cardholder data in accordance with applicable laws as well as compliance with PCI SSC requirements. All merchants must comply with this policy and certify it annually. The risks of noncompliance include substantial fines and penalties imposed on the University by the card associations, liability for all financial losses incurred as a result of a security failure, and damage to the University's reputation.

III. Scope

This policy pertains to certain commercial activities taking place at the university that are unrelated to student tuition/fees handled by the Bursar Office. Examples include: workshop and seminar registrations, merchandise sales, consultation services, and event tickets.

IV. Applicability (Roles and Responsibilities)

All University personnel, departments, and business units involved in collecting credit/debit card payments or handling cardholder data, along with those overseeing Merchant Service Provider applications, are responsible for applying and adhering to this policy.

V. Definitions

Payment Card Industry Data Security Standards (PCI DSS) is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent card fraud through increased controls around data and its exposure to compromise. The standards apply to all organizations that hold, process or pass cardholder information.

Merchant Services Provider (MSP) is a financial software partner that allows the accepting and processing of payments.

Cardholder Data is any personally identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number and Card Validation Code (e.g. the three or four digit number printed on the card, also referred to as the CVV or CVC number).

Merchant ID (MID) is the unique number that identifies each department for transaction processing and accounting.

Point of Sale (POS) is a computer or credit/debit card terminal that either runs a standalone system or connects to a server that processes payments.

eCommerce occurs when the authorization and settlement of a transaction are processed through a computer over the Internet. Typically, the credit/debit card is not present and the customer is offsite with respect to the merchant.

VI. Process

Any University department electing to accept credit/debit cards as a form of payment must complete a TouchNet Store Set Up request form. Touchnet is the university's primary credit/debit card point-of-sale system, and should be used unless the vendor's applications are not compatible with Touchnet. In those circumstances, one of the university's other two point-of-sale systems, Clover or Stripe, should be utilized.

The TouchNet Store Set Up request form must be approved by both the department's Division leadership and the Budget Office. Upon approval, FSI staff will meet with the department to review the request, including the best fit MSP provider, and the development of a test application will commence. After the test application is approved by the applicant department for production it will be replicated in production, tested again and then deployed. All individuals responsible for processing, managing and reconciling transactions must read the Store Manager's Guide to PCI Compliance: Dos and Don'ts available at this link: here.

The applicant department is responsible for all credit/debit card processing fees as well as all costs associated with credit/debit card processing equipment. The processing fees imposed by the card brands (Visa, Mastercard, Discover, and American Express) generally range from 2.0% to 2.5% of sales. These fees are assessed based on the type of card presented by the consumer.

The applicant department also plays a crucial role in safeguarding these types of financial activities. Specifically, the applicant department is responsible for the management of the merchant ID account established. Responsibilities include:

All Departments:

- Account reconciliation and reporting
- Timely response to all refund requestsTimely response to customer inquiries

Departments with POS Equipment:

- Maintain a current list and location of terminals and authorized users
- Provide equipment inspection logs for review upon request by auditors
- Maintain the chain of custody records for all equipment that has direct physical interaction with Cardholder data.

Store managers can find the TouchNet store manager task procedures here.

University departments are prohibited from establishing independent banking relationships for card processing. **Mobile Payment Services (e.g., CashApp, Venmo) and online systems (e.g., PayPal, Zelle) are not approved for University transactions.**

V. Compliance and Annual Certification:

University departments accepting payment cards must comply with PCI-DSS Security Standards, requiring annual certification. Non-compliance may lead to fines, forensic examinations, and suspension of processing. Failure to meet policy requirements may result in payment capability suspension, and associated fines become the responsibility of the affected department.