



**Approving University Official(s):** Mandy Distel, Vice President and Chief Financial Officer  
**Responsible Office:** Business and Finance  
**Effective date:** September 1, 2025  
**Next Review Date:** September 1, 2028

## Merchant Card Processing Policy

### Policy Statement

---

In order to accept credit or debit card payments, a Northwestern University (NU) school, department, or organization must:

- receive prior approval from Treasury Operations, and
- ensure that the payment process and related recordkeeping adhere to university accounting guidelines, University policies, the Payment Card Industry Data Security Standard (PCI DSS), and all applicable contractual or legal obligations.

### Reasons for Policy/Purpose

---

1. Credit or debit card transactions are monetary transactions and are subject to the same control and reconciliation policies as cash transactions.
2. Merchant card transactions are governed by university-wide banking agreements; therefore, independent establishment of payment processes may constitute a breach of contract.
3. Improper protection of merchant card data, whether in electronic or paper form, could lead to a breach of our security obligations that may result in
  - a data security incident or breach,
  - fines,
  - legal fees or other notification-related costs,
  - damage to NU's reputation or financial record,
  - customer ill-will,
  - concessionary costs, such as offering credit monitoring to individuals put at risk,
  - other potential damages and consequences for Northwestern as a direct result of violating the rules of PCI-DSS.

### Who Needs to Know This Policy

---

Any NU employee, contractor, business partner, or student involved in the processing of debit or credit card payments or who has authority over a system that accepts, processes, transmits, or stores such payment data

## Definitions

---

e-Commerce	The process of conducting payment transactions over a computer network, usually the Internet. In e-commerce the merchant card is usually not present; instead, the payer enters that data into a web-based form remotely.
Merchant	A department, school, or other NU organization that collects revenue. Although merchants may receive payments in various forms (i.e. cash, check, voucher) this policy applies to merchants who wish to receive at least some of their payments from credit or debit card transactions.
Merchant Card	Debit or credit cards, including those under the Visa, MasterCard, Discover Card and American Express brands.
Merchant ID	A merchant identification code or merchant account assigned by the bank and is used to identify the owner of merchant card transactions.
P2PE	Point-to-Point Encryption security technology that has been validated by the PCI Council to secure Payment Card information by converting the data into tokens. This secure technology reduces the PCI compliance requirements and risks associated accepting, processing, transmitting, or storing Payment Card information. A list of PCI Validated P2PE Solutions can be found at <a href="https://www.pcisecuritystandards.org/assessors">https://www.pcisecuritystandards.org/assessors</a> and solutions/point to point encryption solutions.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) defines security requirements for card transactions and is required by a consortium of card providers (i.e., Visa, Master Card, Discover, and American Express). Failure to comply with PCI DSS may result in substantial fines, increased auditing requirements if a breach occurs, and the potential of losing the ability to process Payment Cards. The full text of the standard and other supporting documents are available at <a href="https://www.pcisecuritystandards.org/">https://www.pcisecuritystandards.org/</a> .
Payment Card	See “Merchant Card.”
Point-of-Sale (POS) System	Point-of-Sale system. A computer-based system that processes payments over a network. A POS system differs from an e-commerce system in that the payer and card are usually present at the time of the transaction when using a POS system.
Terminal	A machine for electronically processing credit card payments. Card data may be captured by swiping, dipping, or tapping the card through a designated slot or interface on the terminal or by keying in the card number by hand. Payment information may be transmitted over phone lines, Wi-Fi, cellular connections, or the University network.
Terminal ID	A unique identifier assigned by the processor to each card accepting device, whether it is a card swipe terminal, POS, or a connection through an e-Commerce gateway.

## Policy Description

---

### Approval to Accept Payment Cards

Any NU entity that wishes to accept debit or credit card payments through any medium (e.g. e-commerce, paper, phone, mail, fax, terminal, or point-of-sale system) must get approval from NU Treasury Operations and use established vendors and processes.

Furthermore, each NU entity that wishes to accept debit or credit card payments must first have a unique merchant identification number. Treasury Operations secures merchant IDs, establishes them with the preferred processor and has them associated with one of the University's bank accounts. Generally, only authorized cash collection units may request to become a card processing merchant.

Merchant card transactions may be processed via e-commerce systems, POS systems, or terminals. A Northwestern New Merchant Account Request Form (<https://www.northwestern.edu/controller/treasury-operations/e-commerce-operations/>) must be submitted to Treasury Operations.

Approvals for requests to accept credit or debit card payments are granted based on several factors including, but not limited to, the following:

- strength of the business case,
- estimated transaction volumes,
- average dollar amount per transaction,
- compliance with PCI DSS requirements,
- whether or not cardholder data and other sensitive information will be stored and/or processed either on the University network or hosted by a PCI DSS compliant third-party service
- solidity of business processes and internal controls around procedures for collecting, recording, and reconciling sales and credits.

Any e-commerce or software-based payment system must have a contract reviewed, approved, and coordinated for signature by Northwestern IT (NUIT). A third-party risk review (or Service Provider Security Assessment) may also be required. Treasury Operations may also require the requesting Unit to provide evidence of other relevant approvals from University offices, for example the Office of General Counsel, as necessary, prior to issuing final approval to take merchant card payments.

Payment card terminals are acquired through Treasury Operations and must be PCI Validated P2PE. Treasury Operations has pre-approved solutions for payment terminals, gateways, POS systems, and e-commerce transactions.

Merchants wishing to accept payments over the phone shall use the University's PCI Pal solution, a University-provided cell phone or an analog telephone line.

Use of any other e-commerce or alternative method of collecting payments via credit or debit cards not listed above is strictly prohibited, without an exception approved in writing by Treasury Operations.

### Centrally Managed Revenues

Centrally managed revenues, such as gifts, grants and tuition are the responsibility of their respective central administrative units. No school or department-based application may solicit or record gifts to the University, sponsored research grants, or tuition for credit courses. The evaluation of tuition payment options for units already taking credit cards will be handled separately from this policy.

## **Types of Cards Accepted**

Visa, MasterCard, American Express, and Discover are the only types of merchant cards authorized for use at the University.

## **Establishing Contract**

All contracts for payment processing systems or services must use NU owned merchant accounts and have prior approval from Treasury Operations, and in some cases the Office of General Counsel. For e-commerce systems, NUIT must also approve security policies and system architecture. This includes agreements for the lease or purchase of software or hardware as well as the outsourcing of any payment system development or management.

In some cases, a third party may suggest or require that payments be processed under that company's Merchant ID rather than one owned by NU. This is not permitted under any circumstances without prior approval for these arrangements obtained from Treasury Operations, who will coordinate with the Office of General Counsel and Northwestern IT as needed.

## **Merchant Card Reconciliation**

A daily accounting of receipts from sales must be balanced against merchant card transactions via daily batch settlement reports. The actual funds for the merchant card transactions are electronically deposited into the university's bank account automatically. All cash handling units are responsible for complying with the [Merchant Card Processing Procedures](#) for developing and maintaining detailed, written departmental reconciliation procedures.

## **Compliance with the PCI Data Security Standard (PCI DSS)**

PCI DSS is an industry-standard set of security controls that is set and monitored by the PCI Security Standards Council <https://www.pcisecuritystandards.org/>. The PCI DSS applies to all merchant card processing and its related recordkeeping, whether electronic or on paper. It is the responsibility of the NU Merchant to read and understand the PCI DSS requirements. Treasury Operations may provide additional guidance.

All merchants must participate in the NU PCI DSS Compliance Program. Some of the requirements are managed centrally, but many require the participation of the Merchant, including:

- Annual completion of a PCI DSS self-assessment questionnaire (SAQ)
- Annual PCI DSS Compliance Training for all staff members who encounter credit card data (even on paper) or use or manage any payment processing solutions.
- Regular physical inspection of payment card processing devices
- Regular information system vulnerability scans or other data security measures, as required by PCIDSS may be required to ensure PCI Compliance.

For full details of the requirements of the program see the [Credit Card Security \(PCI-DSS Compliance\)](#) page on the e-Commerce website.

## **PCI Data Security**

PCI information is considered Level 4 data per Northwestern's Data Classification Policy. PCI data is not permitted on the University network (including taking credit cards over university telephones), and is not permitted to be stored on any university system (including, but not limited to laptops, desktops, mobile phones, or software applications). PCI data may only be transmitted using approved point-to-point encrypted (P2Pe) device or other similar technologies as authorized by Treasury Operations.

## Penalties for Noncompliance

Merchant card processing privileges may be revoked at any time if the merchant fails to adhere to this policy and its related procedures. This includes failing to pay associated fees, failing to complete the annual self- assessment questionnaire accurately, failing to complete annual PCI Compliance Training in the timeframe dictated, failure to pass required vulnerability scans whenever applicable, and failure to attend any other required training.

In the event that a security breach exposes, or is suspected to have exposed sensitive data, the merchant may be responsible for fines, legal fees, notification costs, and concessionary expenses related to the breach. Additionally, the related merchant account may be revoked.

## Responding to a Card-Related Security Breach

In the event that cardholder data may have been accessed by unauthorized persons, please follow the [NU Incident Response Protocol](https://www.it.northwestern.edu/about/policies/incident.html) at <https://www.it.northwestern.edu/about/policies/incident.html>, and notify Treasury Operations immediately via email at [treasury\\_operations@northwestern.edu](mailto:treasury_operations@northwestern.edu). Examples of such incidents include the compromise of electronic information systems as well as loss of paper records.

## Related Information

---

Payment Card Industry Data Security Standard (PCI DSS)  
NU Treasury Operations  
NU Incident Response Protocol  
Data Classification Policy

## Contacts

---

If you have any questions on the policy or procedure for Merchant Card Processing, you may contact Treasury Operations.

Treasury Operations  
619 Clark Street, Room 109  
Evanston, IL 60208  
(847) 467-0422  
[treasury\\_operations@northwestern.edu](mailto:treasury_operations@northwestern.edu)

## History

---

**Origination Date:** July 8, 2008

**Last Amended Date:** September 1, 2025

**Next Review Date:** September, 2028

## Policy URL

---

[https://www.northwestern.edu/controller/treasury-operations/e-commerce-operations/docs/Merchant\\_Card\\_Policy.pdf](https://www.northwestern.edu/controller/treasury-operations/e-commerce-operations/docs/Merchant_Card_Policy.pdf)