UNIVERSITY OF DENVER	UNIVERSITY OF DENVER POLICY MANUAL PCI-DSS COMPLIANCE	
Responsible Department: Office of the Controller **Recommended By:** SVC Business and Financial Affairs, Controller, and Vice Chancellor of Information Technology **Approved By:** Chancellor	**Policy Number** FINA 2.30.070	**Effective Date** 6/15/2026

I. INTRODUCTION

A. The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for data security designed to proactively protect credit cardholder data that has been collected for legitimate business purposes from loss or misuse.

B. The University manages payment card activity to reduce institutional risk and limit exposure to PCI DSS requirements by using approved, PCI-compliant processors and, where feasible, avoiding the storage, processing, or transmission of cardholder data on University-managed systems.

II. POLICY OVERVIEW

A. Payment card data must not be stored, processed, or transmitted on University-managed systems unless explicitly approved by Information Technology.

B. University units that accept payment cards must use approved, PCI-compliant payment solutions and follow University payment processing requirements.

III. PROCESS OVERVIEW

The Office of the Controller and the Office of Information Security are responsible for PCI DSS compliance at the University.

A. Roles and Responsibilities

1. Office of the Controller

a. Evaluates applications for new credit card merchant accounts.
b. Routinely reviews credit card merchant accounts for business need.
c. Notifying the Chief Information Security Officer of any new merchant account(s) approved by the Controller's Office.

d. Provides PCI DSS training to business unit employees associated with e-commerce and\or Point-of-Sale transaction processing.
e. Confirms that there is no unauthorized sharing of POS terminals between business units.

2. Office of Information Security

a. Provides oversight of security and risk considerations related to payment processing.
b. Supports vendor review for alignment with University security standards.

3. Business Units are responsible for:

a. Obtaining approval for merchant account(s) from the Controller's Office.
b. Limiting personnel access to e-commerce and\or POS processes to individuals who have completed PCI DSS training.
c. Attend a Controller's Office training session each year.
d. Implementing measures to prevent unauthorized sharing of POS terminals between business units.
Maintaining proper security for credit cardholder data.

IV. DEFINITIONS

A. "Payment Card" means any credit, debit, or prepaid card, including physical, magnetic-stripe, or chip-based, bearing the logo of one of the five PCI SSC founding members (American Express, Discover, JCB, Mastercard, or Visa).

B. "Payment Card Industry Data Security Standard (PCI DSS)" means the mandatory global security framework designed to protect cardholder data during processing, storage, or transmission. Information on the PCI DSS may be found on the PCI Security Standards Council website: https://www.pcisecuritystandards.org/standards/pci-dss/.

C. "POS" means point of sale.

Revision Effective Date	Purpose
6/8/2018	*Policy posted to Policy Library (update to prior adoption version from 4.15.2011)*
6/30/2021	*Minor revisions to change title and update processes*
6/15/2026	*Revisions to update policy to align with practice*