UNIVERSITY OF DENVER
POLICY MANUAL
PCI-DSS COMPLIANCE

<u>Responsible Department</u>: Controller's Office	**<u>Policy Number</u>**
<u>Recommended By</u>: Provost, SVC Business and Financial Affairs	FINA 2.30.070
<u>Approved By</u>: Chancellor	

I. INTRODUCTION

It is University policy to be in compliance with *The Payment Card Industry Data Security Standard (*PCI DSS*)* requirements for its e-commerce and\or Point-of-Sale (POS) transaction processing activities. The PCI DSS is a set of comprehensive requirements for data security designed to proactively protect credit cardholder data that has been collected for legitimate University business from loss or misuse. Failure to comply with these standards could result in fines and/or the loss of credit card processing abilities.

II. POLICY OVERVIEW

Any University entity that collects, processes, stores, or transmits credit card information needs to adhere to this Policy and incorporate this Policy into its business practices and procedures.

III. PROCESS OVERVIEW

A. Technology Services

Install and maintain a secure network to include firewall configurations that protect credit cardholder data. If any credit cardholder data is stored, it must be stored within an adequately secured network zone. The University shall encrypt transmitted credit card information as required by PCI DSS and maintain a Vulnerability Management Program to include:

1. Business practices that test and verify network connections and any subsequent changes to the network configuration;

2. Define, document, and implement network roles and responsibilities;

3. Require that default passwords on applications and computer systems be changed before being put into service, and implement a reasonable password management methodology;

business units.

4. Maintain proper security for credit cardholder data. Do not transmit or store credit card data (in hard copy or electronic form) in unsecured environments. All exceptions to storing of credit cardholder data must be documented and approved by Chief Information Security Officer.

5. Ensure compliance with PCI DSS policies and practices. Conduct routine self-assessments of e-commerce and\or POS processing business practices.

6. Conduct credit background checks on employees involved in cash transactions, e-commerce and\or POS processes.

IV. DEFINITIONS

None

Revision Effective Date	**Purpose**
6/30 /2021	*Minor revisions to change title and update processes*