UNIVERSITY OF DENVER POLICY MANUAL CREDIT CARD SECURITY

Responsible Department: Controller's Office **Recommended By:** Provost, VC Business and Financial Affairs **Approved By:** Chancellor	**Policy Number** 2.30.070	**Effective Date** 6/8/2018

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;

4. Securely dispose of sensitive credit card information (shredding, pulping, secure wiping of electronic media) to include disposal of POS terminals;

5. Conduct routine self-assessments of business practices and network security, as well as, manage third party testing/assessment of PCI DSS features;

6. Create an incident response plan to be implemented in the event of system breach; and

7. Assist business units with self-assessments.

B. Controller's Office

1. Evaluate applications for new credit card merchant accounts. Routinely review credit card merchant accounts for business need.

2. Monitor and document third party credit card processors and software applications for compliance with PCI DSS requirements.

3. Maintain business relationships with credit card processors and merchant banks.

4. Provide PCI DSS training to business unit employees associated with e-commerce and\or Point-of-Sale transaction processing.

5. Assist business units with self-assessments.

C. Business Unit

1. Obtain approval for merchant accounts from the Controller's Office. Business units are prohibited from negotiating or obtaining individual contracts with outside merchant processors. All outside merchant processors must meet PCI DSS standards.

2. Limit personnel access to e-commerce and\or POS processes to those with proper knowledge and training. Document which employees have access to the e-commerce or POS systems. Attend a Controller's Office training session each year.

3. Prohibit sharing of POS terminals between 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. Before storing any sensitive credit cardholder data, discuss the business reasons with the Chief Information Security Officer. All exceptions to storing of credit cardholder data must be documented and approved by Information Technology, and the business unit.

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