UNM | Policy Office

Draft of 10-14-15/no track changes version 11-17-15

Administrative Policies and Procedures Manual - Policy 7215: Credit Card Processing

Date Originally Issued: 07-01-2010

Authorized by Regents' Policy 7.9 ("Property Management")
Process Owners: University Controller (Main Campus); Senior Executive Officer For Finance and Administration, Health Sciences Center; and Main Campus and Health Sciences Center Chief Information Officers

1. General

The University of New Mexico is committed to protecting against exposure and possible theft of personally identifiable information associated with UNM credit card processing, and to complying with the most recent version of the Payment Card Industry (PCI) Data Security Standards (PCI-DSS) and all other relevant PCI standards. This policy provides requirements and guidance for all credit card processing activities at UNM. All departments that store, process, transmit, or otherwise have access to consumer cardholder data, in full or truncated, are subject to this policy.

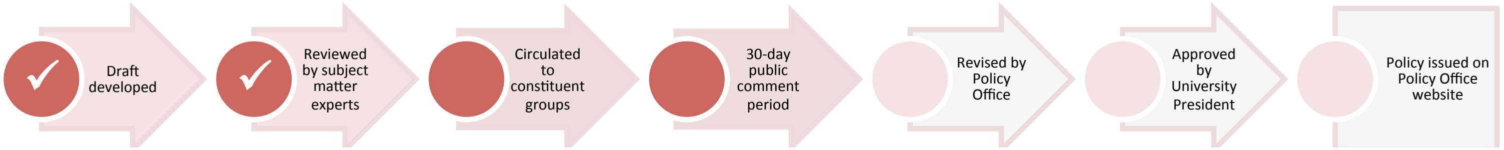
2. Accepting Credit Card Payments

Departments wishing to accept credit card payments must request approval in accordance with Section 3.2.4 of UAP 7200 ("Cash Management") and must comply with all requirements of that policy. Before a merchant ID (MID) number or customer account number (CAN) will be issued, a compliant implementation plan for the cardholder data environment must be provided to and approved, as appropriate, by the University Controller and the Main Campus Chief Information Office (CIO) or by the Senior Executive Officer For Finance and Administration, Health Sciences Center (HSC) and the HSC CIO.

All individuals who store, process, transmit, or otherwise have access to consumer cardholder data, must take UNM Cash Management training and PCI training.

3. PCI DSS Requirements

UNM Information Technologies (IT) and the University Controller will assist departments that


✓
Draft developed
✓
Reviewed by subject matter experts
Circulated to constituent groups
30-day public comment period
Revised by Policy Office
Approved by University President
Policy issued on Policy Office website

process credit cards, or who have access to cardholder data, in complying with the PCI DSS. All computers, networks, and any devices connected to those computers or networks that store, process, transmit, or otherwise have access to cardholder data must comply with the PCI DSS, and with other relevant PCI Standards. The most current applicable version of PCI standards must always be used to measure compliance. Please check the PCI Standards Council web site for the current list of administrative, physical, and technical safeguards at www.pcisecuritystandards.org.

Departments that process cards, or that otherwise have access to the cardholder data environment, must:

- Never store CVC/CVV/CSC/CVV2 numbers;
- Never store credit card numbers or Primary Account Numbers (PAN)--this is an industry standard term--except for the last four digits;
- Never e-mail cardholder data and never use electronic messaging or texting systems to store, transmit, or process cardholder data; and
- Ensure that all third party providers of PCI-related services to the department be compliant with the current version of PCI-DSS and with all other relevant PCI standards.

4. Compliance

Departments responsible for credit card processing must maintain accurate documentation of their cardholder data environment and PCI compliance activities, including, but not limited to, current cardholder data flow diagrams, authorized devices and locations where those devices are securely stored, and all related policies, processes, and procedures.

Departments must also create, maintain, and test business continuity, disaster recovery plans, and security incident response plans annually.

5. Exceptions

Any exceptions to this policy must be approved in writing and in advance, by the University Controller and the Main Campus CIO (for Main Campus exceptions) or by the Senior Executive Officer For Finance and Administration, HSC and the HSC CIO (for HSC exceptions).