THE UNIVERSITY of NEW MEXICO | **University Business Policies and Procedures Manual**

7215
CREDIT CARD PROCESSING

Effective Date: 07/01/10
Subject to Change Without Notice

Authorized by Regents' Policy 7.9 "Property Management"
Process Owner: Vice President for Finance

1. General

The University of New Mexico (UNM) is committed to protecting against exposure and possible theft of account and personal cardholder information and compliance with the Payment Card Industry's Data Security Standards (PCI). This policy provides requirements and guidance for all credit card processing activities at UNM. All departments that use POS terminals handling credit card numbers, in full or truncated, and all departments that maintain servers receiving, storing, or transmitting credit card numbers, in full or truncated, are subject to this policy. An exemption is provided for PCard numbers issued through the UNM Purchasing Department provided the credit card number is functionally truncated to four digits or less.

2. Accepting Credit Card Payments

Departments wishing to accept credit card payments must request approval in accordance with Section 3.2.4. **"Cash Management," Policy 7200, UBP**, and comply with all requirements listed in Policy 7200. All employees and volunteers who handle and/or process credit card numbers must take the cash management training course offered by the University Employee and Organizational Development Department.

3. PCI Technology Requirements

UNM Information Technologies (IT) will assist departments in complying with the technical requirements of this policy. All computers and computer networks handling credit card numbers must comply with the Payment Card Industry's Data Security Standard and, minimally have the following in place.

3.1. Computer System Security Requirements

All computers and servers handling and processing card numbers must be approved by and registered with Information Technologies (IT). All computers and computer networks handling credit card numbers must have the following in place:

- a host-based firewall technology preventing connections from all ports except a specific subset;
- anti-virus software used daily with up-to-date patches;
- file integrity monitoring to an external system for critical system and application files for inappropriate/unauthorized modifications with daily reviews;
- system logging or auditing to an external server for all critical operating system modification;

- up-to-date operating system and application software security patches; and
- access is allowed only by using uniquely assigned and auditable IDs.

3.2. Connectivity Security Requirements

All computers handling credit card numbers must have the following provisions in place for network and modem connectivity:

- a network-based firewall preventing inappropriate/unauthorized access from outside the department or specific authorized computers;
- an intrusion detection system monitoring for unauthorized access attempts;
- monitoring for network-based firewall and IDs systems for potential penetrations;
- specific authorization for modem connections with all modem connection limited to outbound only; and
- all data transfers and administrative access must be in an encrypted format.

3.3. Credit Card Number Storage Requirements

Credit card numbers must be protected by encryption, hashing, or truncation. No complete credit card numbers will be stored on computers in an unprotected manner.

3.4. Physical Security Requirements

All servers storing credit card numbers must have the following provisions in place:

- servers must be secured in a locked room with access limited to system administrators specially approved for access to credit card numbers or escorted by an employee with access approval;
- all access to servers must be logged; and
- backup media must be secured on site, off site, and in transit with transportation handled by approved employees or bonded couriers.

3.5. Outsource Requirements

If credit card processing is outsourced, the contractor must comply with all applicable PCI standards. Software vendors must be certified to be in compliance with the Payment Applications - Data Security Standard (PA-DSS)

3.6. System Audits

Each department responsible for credit card processing must complete quarterly audits on all systems storing or processing credit card numbers to ensure compliance with this policy and **"Cash Management," Policy 7200, UBP**. Information Technologies (IT) will participate in these quarterly audits and will conduct annual audits to confirm the results of the quarterly audits.

Departments must also create, maintain, and test business continuity/disaster recovery plans and system compromise response plans annually.

4. Exceptions

Any exceptions to this policy must be approved by the Executive Project Director of Credit Collections and Merchant Services Department and the Director of IT Security.

Comments may be sent to UBPPM@UNM.edu
http://www.unm.edu/~ubppm

Contents | Section 7000 Contents | Policy Listing | Forms | Index | UBP Manual Homepage | UBP Homepage | UNM Homepage