**THE CONTROLLER’S OFFICE**

**MERCHANT SERVICES POLICY DOCUMENT AND**

 **APPLICATION PROCEDURE**

**Departments requesting a merchant account is required to:**

1. Complete pages 1 and 5 of this document.
2. Complete Wells Fargo Form Requirement
3. Return both (1) and (2) above to the Controller’s office via email generalaccounting-group@unlv.edu

Questions: Call or email generalaccounting-group@unlv.edu Telephone: 702-895-3957

**Describe Business Purpose:**

|  |
| --- |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|   |
|  |

**Provide where you want to post your transaction?**

Department Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

Program (PGxxxxx & Name): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_

Ledger/RC Code: \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_

**Overview**

The Controller’s Office has overall responsibility for the administration and oversight of all banking services (including credit card services). Banking services include the following.

* Set up merchant accounts for various departments;
* Review and approve banking equipment requests;
	+ OIT sets up the equipment once approved.
* Act as the single point of contact between the bank and the various departments and
* Correct recording of credit card activity in Workday.

The Controller’s Office allows departments as merchants to accept the following credit cards:

a. Visa

b. MasterCard

c. Discover

 d. American Express

**Merchant Security Requirements – *Most important: This process is completed by the Office of Information Technology.***

***THE CONTROLLER’S OFFICE WILL SUBMIT THE DEPARTMENTS’ APPLICATION TO OIT FOR PCI APPROVAL***

***The Payment Card Industry Data Security Standards (PCI DSS) is the set of standards for companies (of any size) that accept credit card transactions.***

All merchants must ascertain that it has the ability to comply with the PCI Data Security Standard. Merchants who fail to maintain compliance with the PCI Data Security Standard will have their merchant number inactivated and will no longer be able to accept credit card payments. In addition to the PCI security standards, proper internal controls must be in place that enhances loss prevention. Later in this document, internal controls are addressed. All Merchants must be PCI compliant and are responsible for ensuring the compliance of their unit and any third-party service providers. Merchants must require their third-party provider to sign an agreement stating that they meet PCI security standards and that the third-party provider is liable for any fines which result from a security breach.

Merchants **must keep on file a valid certificate of compliance from their service** **provider**. These standards apply to all payment methods, including retail, mail/telephone order, and e-commerce. These standards are also applicable to non-UNLV entities that are using UNLV systems to process transactions.

**The PCI Data Security Standard identifies 12 basic requirements grouped into six categories.**

**Build and Maintain a Secure Network**

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

 **Protect Cardholder Data**

1. Protect stored data
2. Encrypt transmission of cardholder data and sensitive information across public networks

**Maintain a Vulnerability Management Program**

1. Use and regularly update anti-virus software
2. Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

1. Restrict access to data by business need-to-know
2. Assign a unique ID to each person with computer access
3. Restrict physical access to cardholder data

 **Regularly Monitor and Test Networks**

1. Track and monitor all access to network resources and cardholder data
2. Regularly test security systems and processes

 **Maintain an information security policy**

1. Maintain a policy that addresses information security

**IMPORTANT** - Departments are not allowed to store electronically cardholder data on any UNLV System. This includes, but is not limited to, computers, servers, laptops and flash drives

 Security Breach

A security breach is the unauthorized access of cardholder data, which includes:

Loss, theft and /or fraud.

 An example of a breach would be the theft of credit card receipts that contain the full credit card number. If a merchant experiences or suspects a breach of their merchant account, they MUST immediately notify and provide all details to the Controller’s Office.

Email: generalaccounting-group@unlv.edu
Telephone: 702-895-3957

**Internal Controls**

Internal Controls include authorized staff and segregation of duties. Internal controls provide important benefits to departments and reduces the possibility of mismanagement, error and fraud. Segregation of duties is the cornerstone of internal control. It is a coordinated system of checks and balances in which tasks necessary to complete a transaction either are performed by different individuals, two or more individuals working in tandem, or the tasks are independently reviewed. No one individual should control all aspects of processing a credit card transaction or refund (i.e., reviewing daily batches, reconciling the Statement of Activity and Monthly Merchant Statement). Departments should prepare a written internal control plan for their departmental records. An internal control plan is a description of how a department expects to meet its various goals and objectives by using policies and procedures to minimize the risks. Documenting policies and procedures will clearly communicate specific responsibilities to individual staff, facilitate training new staff, and enable departments to review and monitor their internal control system.

**Authorized Department Staff**

The department contact is responsible for maintaining a current listing of all individuals authorized to be involved in the credit card process in Workday.

The undersigned agree to follow the rules and regulations stated in this Merchant Services Policy document. Any deviations may result in termination of Department as a credit card processing merchant. The Department “Credit Card Merchant Contact” is responsible for the training of their individual staff in accordance with this Merchant Services Policy document. IT Contact responsible for setting up e-Commerce/PC Processing (only required for merchants processing online or using credit card processing software).

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Print)

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Below to be completed by the Controller’s Office:**

Sign: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Chris Viton**
Associate Vice President, Financial Services and Controller
University of Nevada, Las Vegas

Processed by Staff:

Print: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_