General Responsibilities for All Departments utilizing Merchant Accounts

All Payment Card Transaction Types

Comply with applicable sections of the Payment Card Industry (PCI) Data Security Standards (DSS). Comply with the applicable provisions of the current PCI DSS found on the following website. https://www.pcisecuritystandards.org/

New merchants or new purchases - Approval by the Controller's Office before entering into any contract, purchase, acquisition, or replacement of equipment, software, Internet provider, or wireless device that processes payment card transactions.

Maintain a department information security policy – Departments utilizing payment card merchant accounts must establish policies and procedures for physically and electronically safeguarding cardholder data. **(Please use the form titled "Responsibilities of Payment Card Handlers and Processors" (Appendix A) and make the necessary additions pertaining to your department's payment card processing arrangement.)** (PCI DSS 12)

Prevent unauthorized access to cardholder data and secure the data – Establish procedures to prevent access to cardholder data in all forms including but not limited to the following: hard copy or media containing payment card information must be stored in a locked drawer or office; department should establish password protection on computers; visitor

Over the Counter Transactions

Verify signature of cardholder at the time of the transaction.

Obtain the signature of the cardholder on the receipt and provide the duplicate copy to the cardholder.

Be sure only the last four digits of the card number are printed on the receipt.

Store the departmental copy of the receipt safely until it is needed for end of day balancing.

Keep all receipts for each day together. Compare them to daily totals and then group them with the daily batch settlement tape for storage/reference purposes.

Record the batch total and batch number for each day in the monthly summary report.

If for any reason the terminal does not work, use the standardized payment form and provide the bottom portion as the cardholder's receipt. Include a description of the transaction, the transaction date, and the dollar amount on the portion signed by cardholder and give them a copy for their records. Hand enter when the terminal is running again. Keep the original copy of the form and destroy validation code immediately after processing in a manner that will render them unreadable (crosscut shredding or third-party shred bin).

Log and inspect terminal or card swipe mechanism to ensure it has not been tampered with and is working properly.

- Daily for publicly accessible readers or devices used infrequently, weekly for supervised readers that may have exposure to public or non-PCI staff, and monthly for those located in a secure office.

Terminal or card swipe mechanism must be stored securely overnight.

Mail-in, FAX and Phone Orders

Maintain a payment listing for balancing and accounting purposes. This listing should not contain the cardholder data –the last four digits of the card number may be listed.

FAX machines must be a secure analog standalone

APPENDIX A
Responsibilities of
Payment Card Handlers and Processors

As an individual person involved in the handling of cardholder data, I agree to abide by the provisions in this document. If I need further clarification, I will refer to UNLV Payment Card Merchant Policy.

I will NOTwill will documen1C1.3C)2.’6 ( )0cess4 0 Td( )Tw 1.142 0 Td(will)Tj0043 0 Td( )Td Tc 0.01(r)-w 1(f)8