Controller's Office Procedures – Requirements for Payment Card Processing

The requirement to follow these procedures is specified in University Policy 120, the Payment Card Processing Policy.

I. Definitions:

a. "Payment Card" shall refer to any of a range of different cards that can be used by a customer to make a payment, but does not include the University's declining balance cards.
b. EMV stands for EMV stands for Europay, Mastercard, and Visa. The term refers to payment cards with chips embedded in them.
c. P2PE stands for point-to-point encryption, a payment security solution that instantaneously converts confidential credit card data and information into indecipherable code at the swipe of the card to prevent hacking and fraud.

II. Approved Payment Card Processing Equipment

Payment cards may only be processed using approved equipment and applications (unless the equipment pre-dates this document and is currently in use). The following types of equipment and applications may be considered for approval:

a. EMV-compatible network, analog or cellular point-of-sale (POS) terminals purchased or leased through the Controller's office;
b. Web-based applications approved by the Controller's office with EMV-compatible P2PE card readers (if needed);
c. A local-area network application, approved by the Controller's office, utilizing EMV-compatible P2PE card readers.

III. Requirements for Processing Payment Card Data:

a. Redact all but the last four digits of the account number and the entire CSV code after running the payment card. Do not store the card-validation code (the three digit value printed on the signature panel of a card) in any manner.
b. Payment card information must not be transmitted electronically via email, text messaging or any other similar method. If you receive an email containing payment card information, do not process the payment card transaction. You must delete the email and empty from the "Deleted Items" folder and contact the sender to tell the sender how the transaction can be completed. Do not reply to the message with the cardholder data included.
c. Cardholder data handwritten on paper or received by fax must be processed and shredded immediately. You cannot store or transport payment card information on paper to process at a later date.
d. Cardholder data must be protected by multiple layers of security such as a locked office and locked file cabinets.
e. All Point-of-Sale (POS) payment card machines that store cardholder data must be inventoried and properly secured as is cardholder data. All POS machines no longer in use should be returned to the Bursar for destruction.
f. All POS payment card machines should be settled daily thereby clearing the cache of all card data.
g. The merchant copy of receipts shall be kept for 3 years.
h. Cardholder data must be cross-cut shredded before disposal.