Security Guidelines for Handling Credit Card Information

Compliance with Payment Card Industry Data Security Standards (PCI DSS) is required. An event of data exposure may result in significant fines for the University. Departments that are provided with equipment that will allow them to process credit card data are identified in this document as terminal merchants. In addition to terminal merchants, departments may also take credit card information manually through walk in traffic, telephone or fax. Each department that handles credit card information shall identify an employee in the unit who will oversee credit card processing to assure credit card data is limited to authorized staff and credit card security procedures listed below are being followed.

- You can accept cardholder data by telephone, mail, secure non-networked fax or in person only. Do not solicit payment card data by e-mail, unsecure web form, fax server, or network attached fax, as this is not safe.
- All face-to-face transactions should have the payment card present and obtain a signature. Always verify that the card is valid and signed. Compare signatures and check for ID where possible and feasible.
- When it is necessary to store cardholder data prior to processing the transaction, it must be stored in a "secure" environment.
    - The department shall purchase a lock-box or other security device to hold paper records until they can be processed and disposed of. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is left on someone's desk or in a stack of filing.
    - Departments that accept orders by mail should secure all incoming mail until it is open and cardholder data is separated.
- All documentation containing cardholder data must be destroyed in a manner that will render them unreadable (cross-cut shredded) after the payment has been processed.
- Cardholder and merchant receipts generated from a point-of-sale terminal or paper receipts generated by a department must include only the last four digits of the account number. The expiration date must be excluded.
- Merchant terminals must be closed out daily.
- Access to cardholder information should be limited to only those individuals whose job requires such access.

- Departments are required, in good faith, to maintain a fair policy for the exchange and return of merchandise and for resolving disputes over merchandise and/or services purchased with a payment card. If a transaction is for non-returnable, non-refundable merchandise, this must be indicated on all copies of the sales draft before the cardholder signs it. A copy of your return policy must be displayed in public view.
- Departments should not, under any circumstances, pay any card refund or adjustment to a cardholder in cash. If cash is refunded and the cardholder files a dispute your department will bear the loss of income from the transaction.
- Retain payment data other than credit card information in a secure location for 7 years per record retention guidelines. You may need to restructure your forms so that credit card data is at the bottom and can be separated and destroyed while retaining customer information.
- Wherever possible, storage areas should be protected against destruction or potential damage from physical hazards, like fire or floods.
- Under no circumstances should cardholder data be entered and stored on any computer or database in the department.
- All cardholder data and payment information should be classified as confidential. If it is necessary to send payment data to Financial Services for processing, it should be done by an employee in a locked bag issued by Financial Services.
- Immediately report to the Internal Audit when (a) an unauthorized person is believed to have gained access to cardholder data or (b) a person who is authorized to access cardholder data is suspected of misusing that data.