Credit Card Handling and Acceptance Policy

Scope of the Policy
Credit card companies are requiring merchants who accept credit/debit cards as a means of payment to reduce the risks of exposure to credit card fraud by adhering to specific security requirements, called the PCI Data Security Standards.

This policy will outline the rules for the appropriate handling of credit and debit card transactions and personally identifiable information, including the responsibilities of University employees that process credit card transactions or maintain cardholder information.

Failure to follow this policy will result in the loss of credit card processing privileges by the University.

Definitions/Terms

Credit Card Payment Methods:
1. Secured website (Sentry Secured Services)
2. Mail order
3. Telephone order
4. In person

Credit Cards Accepted:
1. MasterCard
2. Visa
3. Discover

Compliance Requirements:
1. Federal Gramm Leach Bliley Act (GLBA)
2. Payment Card Industry (PCI) Data Security Standards
3. Federal Educational Rights and Privacy Act (FERPA)

Personal Identifiable Information (PII).
1. Cardholder Name
2. Credit Card Number
3. Cardholder Verification Value (CVV2) – the 3 or 4 digit code located on the back of the credit card
4. Address
5. Magnetic Stripe Information

Printed Data
1. Customer Receipts
2. Merchant Duplicate receipts
3. Settlement reports
4. Customer Requisition orders
Policy and Procedure

1. University personnel who receive/process credit card information must properly safeguard the credit card information. This policy applies to all University personnel who receive Personal Identifiable Information (PII) while processing, retaining/storing and disposing credit card data.
   a. Only University personnel are permitted to handle PII data. Student workers are permitted to handle PII, at the discretion of the department and with additional training and certification of knowledge of the policy. Student workers should not be given access to PII data that is stored.
   b. Any employees that are new to departments and permitted to handle credit card transactions will be subject to a criminal and credit background check. The background checks will be performed by the Human Resources department employee designated to administer the background screenings. Any questionable items will be reviewed by the University’s General Counsel for final decision. At the discretion of the Department Head, background checks may be administered on existing employees exhibiting job performance issues.
   c. Employees with access to credit card information must sign the Policy of Ethical Practice via electronic signature, which certifies their understanding and willingness to comply with the Policy of Ethical Practice, and the HR ‘Behavior/Conduct’ and HR ‘Confidential Information’ policy as referenced. Certification is maintained online via the Internal Audit department.

2. All third party vendors software/systems used to process credit/debit card transactions must be compliant with the Payment Card Industry (PCI) Data Security Standards.

3. Departments on campus wanting to accept credit card payments must contact Student Financial Services to determine the best way to allow for their acceptance. In some instances, training on the policies, and proper procedure may apply.

4. Any suspected loss or theft of materials containing PII data must be reported. Employees may notify their immediate supervisor if they suspect a violation or a violation can be reported anonymously, by calling the Reporting Hotline established in the Policy of Ethical Practice.

5. Departments must not retain any credit card information. All credit card and PII submitted on a control sheet will be maintained in Financial Operations. Once processed, any forms that must be retained that include credit card information must have the card number and expiration date rendered unreadable.

6. For departments with approval to process credit cards and retain PII within their department:
   a. Credit card terminals must be settled at the close of business each day. Online credit card transactions are settled automatically at the designated time.
   b. Reconciliations between the settlement reports and bank will be performed by the Controller’s group.
   c. The Controller’s group will handle any ‘chargebacks’ or disputes within the stated deadlines. Supporting documentation from the department originating the charge must be provided (if needed) within the deadline.
   d. PII data must never be released without a legitimate business requirement and management approval.
   e. Only the last 4 digits of the credit card are to be displayed on a receipt.
   f. Never retain the three or four digit validation code (CVV2) or magnetic stripe information, in any form.
g. Access to PII data must be restricted and all data must be safeguarded from fire and theft. PII data must be stored in a secured, access controlled area in a locked container to prevent unintentional or malicious compromise.

h. All PII must be shredded 18 months after the transaction was processed.

i. When merchant services processors or card associations make significant policy or procedural changes, Student Financial Services will notify the departments.

Departmental Procedures

1. All credit card payments received and/or processed by the departments must be supported by appropriate documentation as stated below:
   a. All in-person payments must be supported by the signed copy of the receipt produced by the credit card machine.
   b. All payments received through the mail or by telephone request must have the designated form attached to the University’s receipt. The customer copy of the receipt may be mailed at the request of the individual.
   c. Payments processed through Sentry Secured Services are maintained in Your Pay. Limited access is available within the Controller’s Group.

2. As required by PCI standard, departments processing credit card transactions and maintaining PII must have written procedures that include the following:
   a. Segregation of duties
      In most situations initiating transactions, the daily deposit and the reconciliation to the bank are done by different individuals.
   b. Deposits
      Money is deposited the next working day from when it is processed in the Patriot System. The individual balancing reports are combined into a daily deposit report. Receipts are verified. Credit card payments should match the amounts of the Settlement reports. Any discrepancies are noted and corrected as soon as possible.
   c. Reconciliation procedure
      Bank reconciliation is done on a daily basis, using the deposit report, which includes all credit card transactions.
   d. Physical Security
      All credit information received by Student Financial Services is stored in the Controller’s group file room. The files are locked during the day and keys are restricted. The file room is locked each evening. Any PII not received by Student Financial Services is required to be safeguarded by each department as stated above.
   e. Disposal
      The entire deposit folder is destroyed after 18 months. The deposit folder includes: the deposit report, the individual cash balancing reports, all credit card information, wire transfer information and any other supporting documentation.