MONMOUTH UNIVERSITY
Policies and Procedures

Policy Name: PCI DSS Compliance Policy

Original Issue Date: April 5, 2011

Revision Date: N/A

Issued by: Edward Christensen, Vice President for Information Management
William G. Craig, Vice President for Finance

Approved by: President's Cabinet

I. PURPOSE:

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by the PCI Security Standards Counsel to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. Monmouth University, as a payment card merchant (accepting payment card payments), is required to be in compliance with this standard. Compliance with this standard will help provide our students, donors, and other customers with confidence that the University is doing what is necessary to safeguard their sensitive and personal payment card information. Noncompliance with this standard places the University at risk from potential lawsuits, insurance claims, unwanted publicity and payment card issuer and government fines. The following University PCI DSS Compliance Policy is designed to assure that the University meets and maintains this standard of safekeeping our customers' payment card information.

II. POLICY

A. Cardholder data

1. Cardholder data falling under this policy is any information found on the front or back of a payment card including the complete Primary Account Number (PAN), Expiration Date, the verification code or value (three-digit or four-digit number printed on the front or back of a payment card), Cardholder Name and Address, and any other data contained on any track of the magnetic stripe.

B. Electronic storage of cardholder data

1. No storage of full contents of any track from the magnetic stripe.

2. No storage of the verification code or value.

3. No storage of the identification number (PIN) or the encrypted PIN block.

4. No storage of full Primary Account Number (PAN) is to be stored electronically on any University computer or network resource after the payment card transaction has been processed. Storage of the last four digits of the PAN is allowed in order to confirm that the full PAN provided by the customer for a refund is the same PAN used for the original transaction.

5. Access to systems components and cardholder data must be limited to only those individuals whose jobs require such access.

6. When evaluating vendors of new point-of-sale (POS) systems to be installed or otherwise used on campus, or when designing new POS systems to be developed in-house, assurances must be received that the full PAN will not be stored on any University computer or local network after the payment transaction has been processed. These assurances will be required in the contract or agreement with the University and the software/service provider.

7. All electronic transmission of the full PAN and other cardholder data must be encrypted. No cardholder data should be included in electronic mail or other systems not intended for or certified as PCI compliant.

C. Physical storage of cardholder data

1. Physical storage of the full PAN is allowed until the payment transaction is processed or handed over to a central administration department for processing.

2. The PAN and other cardholder data may be stored temporarily in a secure place until processed, such as a safe, locked cabinet or locked drawer with limited access. Access is limited to only those individuals whose jobs require such access.

3. Once the payment card transaction has been processed or handed over to a central administration department for processing, the PAN (except for the last four digits for refund purposes) must be cross-cut shredded so that the cardholder data cannot be reconstructed.

4. An official Credit Card Authorization Form for physically recording cardholder information for a single payer at a time may be printed from the Cashier's Office webpage. The PAN is located on the bottom of this form to facilitate removal after processing has been completed.

5. An official Credit Card Deposit Form for physically recording cardholder information for multiple payers at a time may also be printed from the Cashier's Office webpage.

The PAN is located along the right side of this form to facilitate removal after processing has been completed.

D. Physical storage of cardholder data when a sequence of payments has been authorized

1. Physical (not electronic) storage of cardholder data may be stored in a secure location, such as a safe, locked cabinet or drawer with limited access, until the last of the sequence of authorized payments is processed.

2. Once the last payment of the authorized sequence of payments has been processed, the PAN (except for the last four digits for refund purposes) must be cross-cut shredded so that the cardholder data cannot be reconstructed.