University of Nebraska at Omaha
Credit Card Information Security Guidelines
For Departments Using Point of Sale (POS) Systems

The following guidelines are to be used by departments when collecting credit card information from individuals in order to process payments for services, purchases, registrations, etc. Please strictly adhere to the following guidelines in order to safeguard credit card information:

- When accepting credit card information for payments where the card is not present, use the UNO "Departmental Credit Card Authorization Form" to document the transaction information if another form has not been developed in the department.

- All POS systems must be approved by the Director of Information Technology Services (ITS) and the Manager of Cashiering/Student Accounts who will review the system for PCI DSS compliance and PABP certification. Any system that does not meet compliance with PCI DSS will not be considered for use on the UNO campus. There will be no exception.

- POS systems must be fully hosted with no credit card data transmitted over a UNO network. If a fully hosted option is not available, data storage/transmission must be encrypted and secured in a manner directed by the Director of ITS. Stored credit card data will only be allowed on the UNO campus on servers designated PCI compliant by ITS.

- Quarterly network scanning is a requirement of PCI DSS on any server or POS that accepts/transmits/stores credit card data. Costs of network scans will be distributed to departments where required.

- Access to credit card account numbers should be restricted to users on a need-to-know basis.

- Accept credit card information by telephone, mail or in person only, NEVER through electronic mail. Accepting credit card information by telephone has more risk since a copy of the authorizing signature is not received for use in potential dispute resolution. It is the department head's choice to accept credit card information by telephone.

- Under no circumstances should credit card information be emailed out of the department.

- When it is necessary to record an entire credit card number on a document in order to process the transaction (for example, cardholder information received via mail), "black out" all but the last 4 digits of the credit card number on the document as soon as refunds and disputes are no longer likely, preferably within 60 days. In no case will the entire number be retained for more than 18 months.

- Store paper records in a locked room or cabinet when unattended.

- Allow only authorized employees to have access to the secure record storage area(s).

- Wherever possible, storage areas should be protected against destruction or potential damage from physical hazards, like fire or floods.

- If cardholder data is compromised, contact the Cashiering/Student Accounts Office immediately.

- The department head is responsible for maintaining internal controls over the department's money collection processes. Recommended controls can be found at http://cashiering.unomaha.edu/faculty_staff.php

- Valuable information is available from VISA on minimizing fraud and other merchant issues at http://usa.visa.com/business/accepting_visa/ops_risk_management/

- The department will be charged a discount fee on all credit card receipts. This fee will be based on charges assessed to UNO by the credit card acquirer on the monthly merchant account bank statement. Any questions regarding the assessment of discount charges should be directed to Accounting Services at x2320.

- Questions regarding credit card security should be directed to Cashiering/Student Accounts, x2324.

Your signature on this form will indicate that you and authorized employees in your department have read, understand and agree to abide by the UNO Credit Card Information Security Guidelines and that any new authorized employees will be immediately trained on the Guidelines.

_____ _____

Signature of Department Head Date

_____

Print or Type Name of Department Head