

Credit Card Processing Procedures

January 13, 2009

Table of Contents

10	<u>Introductions</u>
20	<u>Credit Cards Acceptance and Processing</u>
30	<u>Credit Card Payment Processor</u>
40	<u>Authorization Code for Each Transaction</u>
50	<u>Training on Handling Confidential Information</u>
60	<u>Handling Credit Card Information</u>
70	<u>Payment Industry Card Requirements</u>
80	<u>Chargeback's</u>
90	<u>No Disclosure of Cardholder Information</u>
100	<u>Questions</u>
ATTACHMENTS	
150	<u>Payment Card Industry Data Security Standard</u>

[10 Introduction](#)

This procedure provides guidance concerning the acceptance of credit cards in payment for fees, products and services at the University of North Florida (UNF). UNF has adopted the following procedures to assist departments which accept credit card payments.

[20 Credit Card Acceptance and Processing](#)

The Treasurer's Office will facilitate the acquisition of credit card equipment and assess credit card processing fees to the departments. The department will be responsible for installing any telephone line or data line for the credit card reader, if needed. At the time

the credit card equipment is installed the latest version of the contract vendor's Merchant Operating Guide will be provided to the department on how to use the specific equipment. The acceptance of credit cards does not alter the need of an official receipt or other approved method of issuing a receipt and the depositing of receipts. The department is to submit to the University Cashiers Office daily a batch for the credit card transactions and the summary credit card totals unless a process is used which does this automatically.

All technology implementation associated with the credit card processing must be in accordance with the Payment Card Industry Data Security Standards (PCI DSS), <https://www.pcisecuritystandards.org/>, for more information. The cost of equipment or other related measures for compliance to standards will be the responsibility of the department.

The cost of processing credit cards (Discount Fee) will be paid from departmental funds and the expenditure document will be prepared by the Treasurer's Office for all campus departments. The University is centrally invoiced by the credit card processor and the Treasurer's Office distributes the cost to the department based on the usage of the service.

No employee of the University is to advance any cash to the Cardholder in connection with the card transaction. There should not be any element of credit for any purpose other than payment for a current transaction.

30 Credit Card Payment Processor

The fees for processing credit cards vary according to the type of card and how it is processed. The equipment needed to handle credit cards may be provided by any approved vendor for a fee. The Treasurer's Office will provide assistance to the department in contacting the contract vendor and getting the appropriate equipment and software set up.

The University honors without discrimination valid credit cards properly tendered for use. Each sale the University makes involving a credit card must be evidenced by a single sales data record completed with the sale date and the sale amount, and the information as required by the Associations or by the credit card processor. The University in accordance cannot set a dollar amount above or below which it can refuse to honor otherwise valid cards. In the case of whether the payment is received either by mail, telephone or pre-authorized transaction, it is the responsibility of the University to have reasonable procedures in place to ensure that each card sale is made to a purchaser who actually is the Cardholder or is the authorized user of the Card. The University can not rebut a Chargeback where the card holder disputes making a purchase without an electronic record of the Card.

40 Authorization Code for Each Transaction

For all credit card transactions, authorization/approval codes at the point of sale for all card transactions must be obtained.

50 Training on Handling Confidential Information

Credit card information is protected and considered under the Information Security Plan. References and background checks for new full time employees working in areas that regularly work with covered data (credit cards) and information are to be checked. Casual workers such as students, volunteers, etc. that do not work with covered data (credit cards) regularly need not be checked. All credit card information is to be treated as Highly Sensitive data and is to be handled appropriately. Each employee is to be properly trained on the importance of confidentiality of these records and information. Each employee is to also be trained in the proper use of computer information and passwords, if needed for handling credit card transactions.

Any employee involved with handling credit card information is to sign an Employee Certification on Handling Confidential Information form at the time of employment and as of January 1 each year thereafter. The Controller's Office and the Treasurer's Office are responsible for conducting training sessions for all personnel who work with credit card payments. Please contact the Controller's Office, (904) 620-2448, if you have questions regarding these training sessions.

60 Handling Credit Card Information

All credit card information is to be kept to a minimum. The storage and retention of any credit card information is to be limited to which is required for business, legal and/or regulatory purposes, as documented in the data retention policy. No credit card information is to be retained unless protected in accordance with PCI DSS (<https://www.pcisecuritystandards.org/>).

The receipt printed by the credit card reader/terminal or any other printer is to truncate all the digits of the credit card number except for the last four digits and the expiration date is not to appear on the customer's copy. If the complete number is listed or the expiration date appears on any of the credit cards receipts, the equipment is to be re-programmed or the equipment is to be replaced with equipment that complies with these requirements.

If a credit card number is provided over the telephone or through the mail, only authorized and trained employees on confidential material are to have access to this information and as soon as the transaction is entered into the credit card reader the document that has the credit card number is to be shredded. If the documentation that has the credit card number is required to be retained, the documentation is to be accessible only to employees who are authorized and trained on handling confidential and sensitive information. The documentation is to be secured at all times and stored in a locked and secured area or cabinet with access permitted to only authorized and trained employees.

The use of the three digit security code (CVV2, CVC2) is to be requested on telephone orders to ensure valid card information. The use of Credit Card Terminals which request additional information such as, zip code, security codes and etc. will also save on processing fees.

No credit card information is to be requested to be sent through the email process. Email is not secure in any format and is not to be used.

Most credit card terminals provide for a deposit report and a detailed transaction report at the end of each day from the credit card equipment. The deposit report only provides the number of transactions and the amount necessary for recording and depositing the funds received. A copy of the deposit report is to be forwarded to the University Cashiers Office and a copy is to be retained with the departmental receipt information and the signed copy of each credit card transaction receipt.

If payment was received from the customer by use of a credit card, any refund is to be made only to the customer's credit card. This will ensure the customer does not cancel the original transactions and get a refund through the credit card company and you receive a chargeback for the refund. Refund checks are not an acceptable reimbursement method for credit card sales and will not be accepted as proof of a refund

The daily detailed report from the credit card equipment may provide the complete credit card number and the amount. If it is necessary for balancing purposes to obtain this detail transaction report which lists each transaction at the end of each day, it is to be shredded when the balancing is completed or have the equipment programmed to print only the last four digits of the credit card number. If the complete number is listed, the list is to be made only available to employees authorized and trained on the handling of confidential and sensitive information and properly secured until destroyed.

[70 Payment Card Industry Requirements](#)

The companies of all credit cards which are accepted by the University require all merchants and credit card processors store, transmit or process credit card holder information in compliance with Payment Card Industry requirements. The PCI DSS consist of 12 requirements in pursuit of six goals as listed below:

Build and Maintaining a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Before any department can accept credit cards, these 12 requirements must be in place. Most of these requirements consist of safeguarding information in computer environments. However, some of these requirements are for processing and securing non-computerized applications. Non-compliance to these standards can result in significant fines.

In order to ensure compliance with PCI DSS, departmental fiscal managers must attend a mandatory training session.

Any department handling credit cards through a computer environment is also required to have a quarterly Network Scan completed by the University approved scanning vendor (to be determined at a later date).

80 Chargeback's

The University may receive a chargeback from a Cardholder or card issuer for a failure to issue a refund to a Cardholder upon the return or non-delivery of goods or services, if an authorization codes was required and not obtained, the Sales Data was prepared fraudulently or the cardholder disputes the Card sale.

90 No Disclosure of Cardholder Information

Employees shall exercise reasonable care to prevent disclosure of card information, other than to authorized entities for the purpose of assisting the University in completing a card transaction. The University and its credit card processor will store all media containing card numbers in an area limited to selected personnel and any material containing

Cardholder information will be destroyed in a manner rendering the account number unreadable. If at any time account number information has been compromised, notification is to be made immediately to the University Controller, University Treasurer and Director of Internal Audit.

100 Questions

All questions regarding the processing of credit cards are to be referred to the Controller's Office, (904) 620-2448.

DRAFT