



PROCESSING CREDIT CARD PAYMENTS

PAYMENT CARD INDUSTRY (PCI) SELF-ASSESSMENT QUESTIONNAIRE FOR USING CARD SWIPE TERMINALS

How to complete the questionnaire

The questionnaire is used for University departments that use only card swipe terminals for processing credit card payments. Departments that use PC's for entering credit card information must contact B. C. Worsley at 924-4362 for further instructions.

The questionnaire is divided into sections. Each section focuses on a specific area of security based on the requirements included in the PCI Data Security Standard. For any question where N/A is marked, a brief explanation should be attached (see Addendum at the bottom of the form). Merchants with more than one merchant number should complete a separate questionnaire for each functional area. Please provide all merchant account numbers along with processor and deposit information in the Addendum section at the bottom. PLEASE MAINTAIN A COPY FOR YOUR RECORDS

Contact Information

Name: \_\_\_\_\_ Title or Position: \_\_\_\_\_

Phone: \_\_\_\_\_ Email: \_\_\_\_\_

Department Name: \_\_\_\_\_ Origination Code: \_ \_ \_ \_ \_

Merchant Name: \_\_\_\_\_ Merchant # \_\_\_\_\_

Department URL: \_\_\_\_\_

List POS (point of sale) software in use: \_\_\_\_\_

Please provide a brief description of the goods or services the department or unit sells. \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Signature of individual completing the form

\_\_\_\_\_  
Date Completed

## Section 1 - Secure Network

- 1.1 Is payment card account information entered or stored in a database or internal network (i.e. excel file)?  Yes  No  N/A
- 1.2 Is the terminal process currently in use for credit card processing supported by a Cash Register or software system that manipulates credit card information before transmitting to NOVA?  Yes  No  N/A

If, **YES to either question**, stop and contact B. C. Worsley at 924-4362 for further instructions.

## Section 2 - Protect Cardholder Data

- 2.1 Is sensitive cardholder data security disposed of when no longer needed?  Yes  No  N/A
- 2.2 Are the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) stored in the database, log file or point-of-sale product?  Yes  No  N/A
- 2.3 Is the card-validation code (CVV or CVV2 code) are stored in a database, log files or point of sale product?  Yes  No  N/A
- 2.4 Are all but the last four digits of the account number masked when displaying cardholder data? The first six and last four digits are the maximum number of digits to be displayed.  Yes  No  N/A
- 2.5 Are accounts ever sent by you or the card holder by e-mail and if so, is encryption used in the transmission of account number?  Yes  No  N/A

## Section 3 – Strong Access Control Measures

- 3-1 Is access to payment card account numbers restricted for users on a need-to-know basis?  Yes  No  N/A
- 3.2 Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the area where credit card information is processed or stored?  Yes  No  N/A
- 3.3 Are files and equipment (such as servers, PC workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?  Yes  No  N/A
- 3.4 Is all cardholder data printed on paper or received by fax protected against unauthorized access?  Yes  No  N/A

- 3.5 Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?  Yes  No  N/A
- Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information.
  - Label it as confidential
  - If shipped to another location, make sure that it can be accurately tracked
  - Gain management approval to move data from a secure area
- 3.6 Are all media devices that store cardholder data properly inventoried and securely stored with limited access?  Yes  No  N/A
- 3.7 Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?  Yes  No  N/A
- When destroying, cross-cut shred, incinerate, degauss or purge hardcopy materials.

#### Section 4 – Policy on information security

- 4.1 Are information security policies reviewed at least once a year and reviewed with employees?  Yes  No  N/A

#### Section 5 – Card Acceptance

- 5.1 If a Decline/Pick-up authorization code is received, is the card held and returned to the Issuer?  Yes  No  N/A
- 5.2 If a Code 10 is received, do you always call the Credit Card Authorization Center?  Yes  No  N/A
- 5.3. If suspicious activity is suspected, do you call the Credit Card Authorization Center?  Yes  No  N/A
- 5.4 Do you ensure that all transactions are properly authorized?  Yes  No  N/A
- 5.5 Do you compare the signatures on the back of the card with the sales receipt?  Yes  No  N/A
- 5.6 Do you process refunds/credits only to the card number of the original sale?  Yes  No  N/A
- 5.7 Do you settle all transactions daily?  Yes  No  N/A

