

## PAYMENT CARD MERCHANT SERVICES ACCEPTANCE AGREEMENT

NC State University uses the OSC SECP Master Service Agreement to supply the University departments/units with the option to accept payment cards to sell goods and services to its customers. With this service, the University merchants are subject to, must understand and must comply with all rules, regulations and contractual provisions regarding the handling of payment cards. The regulations include the Payment Card Merchant Services, Payment Card Industry Standards and Card (MC, VISA, AMEX, DISCOVER) Association merchant requirements. These rules and regulations must be adhered to as the department/unit or the University may be subject to severe financial penalties for failure to comply.

In an effort to insure that University merchants understand and comply with the above, all University merchants must agree to and follow the following provisions. These provisions are not intended to be an exhaustive list of all applicable requirements. At a minimum, Campus Merchants should familiarize themselves with REG 07.30.23, the PCI-DSS, PA-DSS (both located online at <https://www.pcisecuritystandards.org>), the Payment Card Merchant Services (<http://policies.ncsu.edu/regulation/reg-07-30-23>) and all supporting standards. Refer to the online glossary at [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_Glossary\\_v3.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf) for definitions of certain terms used in this Agreement.

**Please review and initial after each statement to acknowledge the University requirements. Required signatures at the bottom of the agreement to indicate your intent to comply with PCI-DSS.**

### 1. Receipt of Card Data:

#### a) Point of Sale Terminals/Dial Pay:

- i. Payment card must be dipped or swiped and suggest receipt signed for any goods or services.
- ii. All customer/merchant receipts must not display the Primary Account Number (payment card number) except for the last 4 digits.
- iii. It is prohibited to transmit payment card information (e.g. account numbers, expiration dates, etc) via email.
- iv. If card numbers are obtained through the mail or on paper, the information containing the card numbers must be retained in a secure locked area and must be restricted and/or blocked from view of third party and others without the business need to know.

\_\_\_\_\_ (initial)

#### b) eCommerce:

- i. All electronically captured information must be in an encrypted transport layer security (TSL) that meets the Card Industry Standards with minimum access to cardholder information.
- ii. All eCommerce gateways must be PCI certified and compliant with NC State University security requirements.
- iii. All University merchants must utilize a "hosted order page" service of the gateway or any gateway that does not require that the cardholder information be entered on an order page residing on any University web page nor server. Thereby, insuring that the cardholder information is not obtained, stored nor passes through the University servers.

\_\_\_\_\_ (initial)

c) Software Based Merchants:

- i. The third party vendor application is certified and validated and listed on the VISA Payment Application Best Practices (PABP) validated and certified secure application list or PCI SSC list of PA-DSS Validated Payment Applications which both can be accessed at [http://usa.visa.com/merchants/risk\\_management/cisp\\_payment\\_applications.html](http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html)
- ii. All customer/merchant receipts must not display the card number except for the last 4 digits (truncation).
- iii. Card numbers must not be transmitted via email.
- iv. If card numbers are obtained through the mail or on paper, the information containing the card numbers must be retained in a secure locked area and must be restricted and/or blocked from view of third party and others without the need to know.

\_\_\_\_\_ (initial)

2. Transmission of Payment Card Information:

- a) In addition to restrictions on methods of transmittal in the PCI-DSS, payment card information must **not** be transmitted through the following devices:
  - i. Email
  - ii. Network connected fax machine
  - iii. Non-encrypted network components and servers
  - iv. Cell phones
  - v. Lap top computers
  - vi. IPad
  - vii. Tablets

\_\_\_\_\_ (initial)

3. Storage and Disposal:

- a) Cardholder Information must not be stored on any system, computer, technology device, server, or point of sale device after authorization.
- b) Department point of sale terminals must be settled daily and cleared after settlement.
- c) Any cardholder information in paper format must be stored in a secure (locked) limited access area for a period of time no longer than is necessary to meet document retention of the individual units.
- d) Access to the area which is used to process, transmit or store cardholder data must be restricted to authorized University personnel on a need to know basis. All card holder information must not be physically present at workstations when the employee is not physically present.
- e) Customer/merchant receipt must be truncated. If the merchant utilizes mail in or phone order printed forms that include cardholder information, the personal account number (cc#) and expiration date must be rendered unreadable and unrecoverable except the last four digits after authorization.
- f) Storage of the Card validation code (the three digit value printed on the signature line of the card) is strictly prohibited.

\_\_\_\_\_ (initial)

4. Network and Systems:

- a) All network components, servers and purchased and custom applications that are part of the payment card system must conform to all current PCI-DSS requirements. For more information, visit [www.pcicomplianceguide.org](http://www.pcicomplianceguide.org). An outline of the primary principles and requirements follows. Refer to the PCI-DSS (located online at <https://www.pcisecuritystandards.org>) for the detailed elements of each.
  - i. Building and maintaining a secure network
    1. Install and maintain a firewall configuration to protect data
    2. Do not use vendor supplied defaults for system passwords and other security parameters
  - ii. Protecting Cardholder Data
    1. Protect stored data

- 2. Encrypt transmission of cardholder data and sensitive information across public networks.
- iii. Maintaining a Vulnerability Management Program
  - 1. Use and regularly updated anti-virus software
  - 2. Develop and maintain secure systems and applications.
- iv. Implementing Strong Access Control Measures
  - 1. Restrict access to data by business need to know
  - 2. Assign an unique ID to each person with computer access
  - 3. Restrict physical access to cardholder data
- v. Regularly Monitoring and Testing Networks
  - 1. Track and monitor all access to network resources and cardholder data
  - 2. Regularly test security systems and processes
- vi. Maintain a Department Information Security Departmental Policy that addresses information security standards which follows and meets all University Information Security Standards and PCI-DSS requirements.

\_\_\_\_\_ (initial)

5. Payment Card Industry Standards Program:

- a) Annually, upon direction of the University Controller's Office and Security and Compliance, all merchants must complete the PCI-DSS Self-Assessment Questionnaire appropriate to their operation. All questionnaire assessment fees will be the responsibility of the department. Services will be available to assist Units with completing the questionnaire.
- b) All eCommerce merchants will work with their payment eCommerce gateway providers to perform the appropriate network (external and internal) scans quarterly, semi-annually or annually.
- c) Annual Security Awareness training is required by all parties involved in storing, processing or transmitting cardholder data.

\_\_\_\_\_ (initial)

6. Reconciliation:

- a) The merchant is responsible to review monthly merchant statements for accuracy and report any adjustments needed within 60 days of statement date to the University Controller's Office – Merchant Services

\_\_\_\_\_ (initial)

7. Security Compromise:

- a) To meet the PCI-DSS Bank Card industry provision and requirements, all suspected and/or confirmed security compromises will be reported immediately to University Controller's Office -Merchant Services and Security and Compliance.
- b) Any questions regarding compromise can be directed to University Controller's Office - Merchant Services or Security and Compliance.

\_\_\_\_\_ (initial)

8. Merchant Services:

- a) University Controller's Office - Merchant Services will be notified of any department merchant service changes.
- b) University Controller's Office –Merchant Services will facilitate all equipment rental/leasing/purchasing and return of equipment. Exception may apply with prior approval from Merchant Services.

\_\_\_\_\_ (initial)

9. Applicable Requirements:

- a) I have reviewed REG07.30.23
- b) I have reviewed the Payment Card Industry Data Security Standards (located online at <https://www.pcisecuritystandards.org>).

\_\_\_\_\_ (initial)

I understand and agree to comply with the above:

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

Project Number for Financial Obligations: \_\_\_\_\_

Merchant Business Owner Name: \_\_\_\_\_

Contact Phone and Email: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Department/Unit Head Name: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

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