Data Security Standards Acknowledgement and Agreement

Employee Name (printed): ______________________________________

Department: ________________________________________________

I acknowledge that:

1. My access to private, personal data (including sensitive credit card information) is limited to my need to know based on the function of my job responsibilities at the University.
2. I have completed the PCI DSS Training and understand the responsibility I have to protect and safeguard private credit card information entrusted to me.
3. I have read and understand the Payment (Credit/Debit) Card Processing Standard (http://finance.uncc.edu/resources/policies/payment-credit-debit-card-processing-standard) and the Payment (Credit/Debit) Card Processing Procedures (path: S>Campus Merchants>Helpful Documentation). I will comply with the controls set forth in those documents.
4. I have been informed of the Incident Response Plan and understand that if there is an occurrence when I suspect a breach in credit card security or personal data, I will report it immediately to the appropriate personnel.
5. I understand that any violation of the Data Security Standards listed and agreed to in this acknowledgement form can result in disciplinary action, including dismissal from employment, as well as criminal penalties or civil liability.

Employee Signature: ______________________________________

Date: ______________________________________

Employee E-mail Address: __________________________________

Employee Phone Number: __________________________________

Supervisor’s Name: ______________________________________

Supervisor’s Signature: ____________________________________

Date: ______________________________________

Please note: Original signed form is to be returned to eCommerce, Reese 011B
ECommerce Data Security Agreement Key Points

All merchants are expected to comply with the Payment Card Industry Data Security Standards (PCI DSS). Those standards may be accessed at: [https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml). The 12 core requirements of the Standards are:

- **Build and Maintain a Secure Network**
  - REQUIREMENT 1: Install and maintain a firewall to protect cardholder data
  - REQUIREMENT 2: Do not use vendor-supplied default passwords

- **Protect Cardholder Data**
  - REQUIREMENT 3: Protect stored cardholder data
  - REQUIREMENT 4: Encrypt sensitive information across networks

- **Maintain Vulnerability Management Program**
  - REQUIREMENT 5: Use and regularly update anti-virus software
  - REQUIREMENT 6: Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**
  - REQUIREMENT 7: Restrict access to cardholder data by business need to know
  - REQUIREMENT 8: Assign a unique ID to people with access
  - REQUIREMENT 9: Restrict physical access to cardholder data

- **Regularly Monitor and Test Networks**
  - REQUIREMENT 10: Track and monitor access to network resources/cardholder data
  - REQUIREMENT 11: Regularly test security systems and processes

- **Maintain An Information Security Policy**
  - REQUIREMENT 12: Maintain an information security policy for all personnel

- Payment card information is considered personal financial information and must be secured and treated as confidential.

- The access to payment card information is to be restricted to only those with a business need to know and on a least privilege basis.

- University Departments must not capture, store, or transmit payment card information on UNC Charlotte servers or network. No cardholder data is to be stored on computers, workstations, flash drives, or other media.

- Primary Account Numbers (PANs) are not to be stored after authorization in any format, or on any UNC Charlotte device or network.

- Sensitive authentication data (security code or card verification code, PIN, magnetic stripe) is never to be stored, nor should it be manually displayed in a written form for reference or other purposes.

- Receipts containing truncated PANs (only the last 4 digits of the PAN are displayed) should be retained in a locked secured area with limited access for 2 years. They must then be destroyed according to PCI DSS guidelines unless an official action involving the records has been initiated.

- Credit card information should **never** be e-mailed. It should also not be sent by unsecured fax or over network connected fax machines.

- All payment card transactions must be processed on merchant accounts issued by the eCommerce Department in accordance with the NC Office of the State Controller.

- All payment mechanisms, software, equipment, online processing, and payment processing contracts must be approved by the e-Commerce Department in conjunction with ITS Security and be in compliance with the PCI DSS and/ or the Payment Application Data Security Standards (PA DSS).

- Card transactions are not to be entered on University computers or laptops on behalf of a customer without approval by eCommerce and configuration by ITS. Computer stations within the merchant business operations and immediately outside of those operations must also be approved and properly configured if card transactions can be entered on that equipment. In both situations, the computers are deemed as virtual terminals and must meet processing requirements.

- Any suspected breach, or fraudulent or criminal activity involving payment card data must be reported to ITS Security ([Security@uncc.edu](mailto:Security@uncc.edu)) and the e-Commerce Department without delay.