1. **Purpose**

This policy provides the requirements for all payment (credit/debit) card processing activities at UNCG. It defines the responsibilities of employees, administrative units, organizations, and affiliates that process payment cards on behalf of UNCG or its affiliates. All relevant provisions contained in the Information Security Policy, the Data Classification Policy and the Acceptable Use of Computing and Electronic Resources are applicable and included by reference in this document.

2. **Scope**

This policy applies to all academic units, organizations, affiliates, and employees of UNCG who accept credit/debit card payments for University business.

3. **Definitions and Roles and Responsibilities**

3.1 **Definitions**

PCI Standards: Payment Cards Industry (PCI) standards include:

- Cardholder data may not be stored on any UNCG computer device or network. Never send or request cardholder information via email. Credit card numbers should never be sent via end-user messaging technologies.
- All media (including paper) containing cardholder data must be physically secured and protected against unauthorized access, and properly destroyed when it is no longer needed for business or legal reasons.
- All devices that capture payment card data via direct physical interaction (example: Point-Of-Sale terminal) must be protected against tampering and substitution.
- An accurate and up-to-date list of all such devices must be maintained that includes: the make and model of the device, the location of the device, and the device serial number and terminal ID.
- Device surfaces are periodically inspected to detect tampering.
- Departmental personnel are trained to be aware of procedures to detect and
report tampering or replacement of devices.

- The department is responsible to restrict access to cardholder data on a need to know basis and to ensure that all personnel that interface with payment card activities or cardholder data are aware of the importance of cardholder data security and their responsibility for protection of the cardholder information. For departments that utilize service providers, a list of service providers must be maintained. The user of services providers requires:
  
a. A written agreement must be maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of UNCG, or to the extent that they could impact the security of UNCG’s cardholder data environment.
  
b. The service providers’ PCI DSS compliance should be monitored and verified at least annually. The service provider must be listed as compliant on Visa’s “Global Registry of Service Providers” or on the PCI Security Standards Council’s website.
  
c. Information must be maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the UNCG department.

4. Policy

The Office of the State Controller has established a Master Services Agreement (MSA) with SunTrust Merchant Services. The MSA provides services to eligible state agencies, universities, community colleges, and local units of governments on a statewide enterprise basis, allowing eligible participants to benefit from the leveraging of volume pricing.

Business Affairs has signed a Participation Agreement with the Office of State Controller (OSC) which allows campus departments to participate in the Master Services Agreement with SunTrust for the acceptance of credit cards. UNCG departments are not permitted to contract for credit card services outside of the Master Services Agreement without written approvals from the Vice Chancellor for Finance and Administration, the Vice Chancellor for Information Technology Services, and OSC. All accounts for card processing must be established by the Director of Cashiers and Student Accounts Office through OSC.

UNCG is required to be in compliance with Payment Cards Industry standards, which is referred to as PCI Compliance. All payment transactions must be captured on approved processing systems. UNCG is taking an approach to consolidate vendors and minimize complexity and effort in building interfaces in order to support existing operations and
control exposure. Accordingly, there is a freeze on adding any new credit card processing systems or vendors. Any request for use of a processing system not already in place at UNCG must include an explanation why one of the existing vendors/systems will not work, why UNCG should expend additional resources for the extra work and bear the additional exposure the new system will require.

All Payment (Credit/Debit) Card Processing activities must comply with the state of North Carolina General Statutes (G.S.) and policies. That includes but is not limited to the North Carolina G.S. 147.77 (Daily Deposit Act), NC Office of the State Controller Policy 500.2 (Master Services Agreements for Electronic Payments), 500.11 (Compliance with PCI Data Security Standards) and 500.13 (NC Security and Privacy of Data).

Payment Card Industry (PCI) standards apply to all organizations that process, transmit or store credit cardholder information. The University and all departments that process payment card data have an obligation to adhere to the PCI Standards and must annually certify their continued compliance by submitting the PCI-DSS Self-Assessment Questionnaire (SAQ) appropriate to their credit card activities. In addition, departments must comply with all information security policies established by UNCG Information Technology Services (ITS).

All departments accepting credit cards must maintain compliance with Payment Card Industry (PCI) standards at all times (outlined above in Definitions).

Any costs incurred by a department to become and remain compliant with the PCI Data Security Standards shall be borne by the department. In the event of a breach, all fines and expenses associated with the breach will be borne by the department accepting the credit card that was compromised.

5. **Compliance and Enforcement**

The University Controller is responsible for ensuring compliance with this policy.

6. **Additional Information**

6.1 **Supporting Documents**

- Payment Card Industry Data Security Standard [PCI-DSS]
- Annual PCI Compliance Security Procedures Review (.doc)
6.2 Resources

Information Security Policy
Data Classification Policy
Acceptable Use of Computing and Electronic Resources

6.3 Approval Authority

This policy will be approved by the Interim Associate Vice Chancellor for Finance.

6.4 Contacts for Additional Information and Reporting

● Responsible Executive: Todd Mitchell, Director of Cashiers and Student Accounts Office, (336)334-4959, rtmitche@uncg.edu