### 1. Purpose/Introduction

This procedure provides guidance on how to request permission for credit card acceptance and outlines steps required for related activities.

### 2. Definitions

### 3. Procedural Steps

#### General

All University departments and entities shall process inbound payment (credit/debit) card transactions through approved mechanisms/systems, processors, and equipment. The merchant services provider, which is contracted by the North Carolina Office of the State Controller (NC OSC) and by the University, must be utilized for the processing of payment card transactions.

Any department wishing to accept credit cards must obtain prior administrative approvals before entering into any credit card processing agreements. Any third-party software or services must be Payment Card Industry (PCI) compliant. In addition to UNCG administrative approvals, Office of State Controller approval must be obtained for any services outside of the State’s Master Service Agreement (MSA) with SunTrust.

All departments accepting credit/debit cards must comply with Student Accounts Policy 2 Credit Card Acceptance and Processing.

#### Request for Approval

I. The requesting entity (department, school, etc.) must forward a written request to the appropriate Vice Chancellor or Provost.

The request must include:

1. The business need for which credit card acceptance will be used and acknowledgement that the department agrees to abide by all applicable PCI and MSA rules and regulations.
2. Information about any third-party services to be used.
3. Documentation of anticipated transaction volume and mechanism for card acceptance.
4. The funding source for payment of credit card expenses.

II. The Vice Chancellor or Provost will forward an approved request to the Vice Chancellor for Finance & Administration for Approval.

III. The Vice Chancellor for Finance & Administration will forward an approved request concurrently to Information Technology and to the Department Head for sign-off on the technical application and physical security issues.

Oversight
IV. Once all approvals are obtained, the request will be forwarded to the Director of Cashiers and Student Accounts Office who will assist the Department in requesting a credit card merchant number through the Office of State Controller.

V. The department must notify the Director of Cashiers and Student Accounts Office of the responsible person to contact relative to the department’s credit card administration and PCI compliance matters. Notification must also be made whenever the responsible person changes.

VI. All card processing activities are subject to the Payment Card Industry Data Security Standards (PCI DSS). All university departments accepting credit cards must complete a PCI Self-Assessment Questionnaire and Attestation of Compliance before accepting payment card transactions, each year thereafter upon request, and when significant changes to the card processing environment occur.

VII. All card processing must adhere to the North Carolina General Statutes and applicable policies. NC OSC provides oversight for UNCG payment card processing.

VIII. Information security incidents or concerns should be reported to ITS (6-Tech) and the University Information Security Officer. The UNCG Information Security Incident and Reporting Notification Policy provides guidance regarding action to be taken if a security incident is suspected or confirmed.

Daily Responsibilities
IX. On a daily basis, the department must balance transactions and settle their sales electronically to the merchant services provider. Merchants must also:

- a. Prepare appropriate deposit documentation and submit it to the University Cashiers before the day that the settlement of funds for card transactions is reflected in the banking settlement reports. A separate deposit must be created for each day that a settlement occurs. The transactions are not to be combined on one form for multiple days.
- b. Provide appropriate back-up documentation to substantiate the deposit. A copy of the settlement tape from the POS terminal must be included; and/or, a copy of the gateway batch settlement report (totals reports, not detail) must be included for internet transactions.
- c. Departmental staff are responsible for reconciling the card transaction activity and accurately reporting those amounts to the University Cashiers through the deposit process. The merchant, not the Cashiers Office, is responsible for pulling the settlement reports, and reconciling the amounts. The Cashiers Office will compare the deposit to the bank statement report and inform the merchant of discrepancies. All discrepancies should be resolved within 24 hours so that sales can be posted to the departmental account in the UNCG accounting system on a timely basis.
• d. Access to Client Line reporting systems must be requested by the merchant to the Director of Cashiers and Student Accounts for the purpose of providing the appropriate department personnel with required reports for reconciliation, research, and deposit.

• e. Provide deposit documentation on a timely basis for amounts debited or credited directly to the merchant account due to chargebacks, retrievals, reversals, or other activity which affects the merchant account funds.

X. Departments shall maintain adequate records of sales transactions. Daily sales totals, logs, etc. substantiating revenue should be stored in accordance with state record retention policies.

XI. Reconciliation of all transactions must be performed on a regular basis. Transactions and account charges deposited to the University Cashiers must be reconciled and verified before the deposit is submitted. Supervisory review of accounts reflecting refunds, chargebacks, reversals, and card fees should be conducted regularly.

**Additional Requirements for Point-of-Sale (POS) Transactions**

XII. All Card Present transactions must be captured on equipment approved by and obtained through the Director of the Cashiers Office in conjunction with NC OSC. All card transactions will be processed on equipment compatible with the processing platform of the University's merchant services provider. The University merchant services provider is determined by UNCG in accordance with the NC OSC Merchant Services Agreement.

XIII. POS terminals must be tracked and protected from tampering. Physical access to terminals shall be limited to authorized personnel. If terminals are customer facing, they should be monitored while in use and secured when not in use. Terminals must be inspected for tampering on a regular basis. Any suspicious behavior or indications of device tampering, or substitution should be reported to the Director of Cashiers and Student Accounts and the UNCG Information Security Officer.

4. **Forms, Tools, Etc.**

   **UNCG Information Security Incident and Reporting Notification Policy**

5. **Revision Table**

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Section #</th>
<th>Summary of Changes</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>