INTERNAL POLICIES AND PROCEDURES
Merchant Card Processing

I. POLICY STATEMENT

A. Introduction

The NC Office of the State Controller has issued an E-Commerce Policy entitled, “Maximization of Electronic Payments.” The policy states in part, “When developing agency cash management plans, each state agency shall consider utilizing electronic payments methods, for both outbound and inbound payments….Each agency and university shall consider the feasibility of accepting payments via credit / debit card (merchant cards) when appropriate, considering the volume and frequency of payments received..”

Macon County has determined that it is appropriate to accept merchant cards as an acceptable form of payment for certain types of receipts as described herein. Desirous of developing policies and procedures to ensure compliance with all applicable rules, regulations, and policies associated with merchant cards, the policies and procedures described herein have been adopted.

B. Types of Receipts and Types of Cards Accepted

1) Receipts Accepted: In its normal course of business the agency will accept merchant cards for the following types of receipts:
Tax Bills, Lab Fees, Inspection, Document Fees, Dental Services, Medical Services, Permits.

In the case of multiple divisions within the agency, approval for the acceptance of merchant cards must be obtained from Macon County Finance Director.

The Finance Director may also authorize additional types of receipts to be accepted.

2) Cards Accepted: In its normal course of business the agency will accept merchant cards for the following types of cards. Visa, MasterCard, American Express, and Discover.
Visa, MasterCard, American Express and Discover are only accepted currently at Register of Deeds office and Tax collections. All other locations currently accepts Visa, MasterCard.

Reference is made to OSC’s E-Commerce Policy entitled, “Types of Merchant Cards Accepted.”
http://www.osc.nc.gov/SECP/TypesOfMerchantCardsAccepted.pdf

C. Transaction Fees

No transaction fee (surcharge) will be levied for a face-to-face transaction (card-present). (The practice is prohibited by Visa, but permitted by the other card brands, if pre-approved.) (This requirement applies regardless of the option selected below for card-not-present transactions.)

Transaction fees (convenience fees) may be charged to cover the cost of permitting a person to complete a transaction using a web application or other means of electronic access, in accordance with OSC's E-Commerce Policy entitled, "Charging Transaction Fees," and G.S. 66-58.12. Reference is made to the policy: http://www.osc.nc.gov/Credit_Card/ChargingTransactionFees.pdf.

The practice of charging transactions fees shall not conflict with any merchant card associations' Rules. Reference is made to the Rules: http://www.ncosc.net/SECP/ConvenienceFees_and_SurchargeRules.pdf

Convenience fees levied and collected will be retained by a third-party vendor, with the vendor acting as the merchant for that portion of the transaction amount.

D. Funding to Pay Costs

Agency shall adhere to all requirements pertaining to the securing of funding to pay for costs associated with processing merchant cards, including internal costs and costs paid to third-party processors.

Reference is made to OSC's E-Commerce Policy entitled, "Funding for Electronic Payments." http://www.osc.nc.gov/Credit_Card/FundingforElectronicPaymentServices.pdf

E. Methods of Capture

Transactions are normally of two types: "Card present" or "card not-present."
The following methods of capture shall be used:

- Internet application – hosted by third-party, PayPal, Sturgis, BIS
- POS terminals – Stand-alone (Analog telephone lines)
- POS terminals – POS software (Maintained on a network)

F. Third-Party Service Providers

1) Merchant Card Processing Services

The State of North Carolina has a Master Services Agreement (MSA) with SunTrust Merchant Services (STMS), which is affiliated with First Data Merchant Services (FDMS). STMS provides merchant card payment processing services to state and local government entities on a statewide enterprise basis.

On August 28, 2015 agency obtained approval to participate in the Office of the State Controller's (OSC) Master Services Agreement (MSA) with STMS, as required by OSC's E-Commerce policy entitled, "Master Services Agreements for Electronic Payments." Accordingly, the County Manager executed an Agency Participation Agreement (APA) allowing the agency to subscribe to the MSA as a "participant." The APA was reviewed before execution by the agency's management, and management is aware of the responsibilities and obligations required by the terms of the APA, and by reference, the terms of the MSA. The agency's copy of the executed APA is filed in the office of Finance Director.

(If agency has obtained an exemption from participating in OSC's MSA, specify date of exemption.)
http://www.osc.nc.gov/Credit_Card/MasterServicesAgreementsForElectronicPayments.pdf

2) Payment Gateway Services

A third-party gateway service provider may be utilized, provided it is one pre-approved by OSC. Some gateway providers offer a capture solution that also has a "presentment engine" (in addition to the "payment gateway), which provides hosting of the agency's website. Some gateway providers cannot use SunTrust Merchant Services as the processor / acquirer, but use their own processor / acquirer. Third party payment gateway services are provided by PayPal, BIS, and Sturgis.

3) Payment Applications

Capture solutions utilizing POS Software applications are obtained from vendors that have had the application (version utilized) validated as being compliant with the PCI Payment Application Data Security Standard (PCI PA-DSS), formerly known as Visa's "Payment Application Best Practice" (PABP). The payment application must be listed either on Visa's "List of Validated Payment Applications," or on the PCI Council's website:
https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
http://usa.visa.com/download/merchants/validated_payment_applications.pdf

4) Proprietary Card Companies

Participants desiring to accept proprietary cards (e.g., American Express, Discover) must either enter into an agreement directly with each proprietary card company, or enter into a master agreement that the OSC may have with the company. Reference is made to OSC's E-Commerce Policy entitled, "Types of Merchant Cards Accepted." http://www.osc.nc.gov/SECP/TypesOfMerchantCardsAccepted.pdf

On December 2014, the Macon County Finance Director executed an Agency Participation Agreement (APA) allowing the agency to subscribe to the Master Agreement with OSC as a "participant." The APA was reviewed before execution by the agency's management, and management is aware of the responsibilities and obligations required by the terms of the APA, and by reference, the terms of the Master Agreement. The agency's copy of the executed APA is filed in the office of County Manager.
http://www.osc.nc.gov/SECP/SECP_MerchantCard_Master_Services_Agreement.html

G. Data and System Security:

1) PCI DSS Compliance: Each of the merchant card associations has established security standards that all merchants and processors must follow to ensure that cardholder data, as well as the payment network, is protected and kept secure. The standards are referred to collectively as the "Payment Card Industry Data Security Standard (PCI DSS)," which has been issued by the PCI Security Council. The primary focus of the PCI DSS is to help merchants (agencies) improve the security of cardholder information by improving overall security standards which reduces the chances of security breaches. The policies and resulting procedures are intended to help ensure that cardholder data and the electronic commerce network are protected and kept secure, thereby avoiding potential fines. More information is available on OSC's SECP Website: http://www.osc.nc.gov/programs/risk_mitigation_pci.html.

The most useful document to view is: "PCI Applicability to Capture Methods." http://www.osc.nc.gov/programs/pci/PCI_Applicability_to_Capture_Methods.pdf.

Agency will take all necessary steps to ensure that all merchant card applications (merchant numbers) used by the agency are kept compliant with the PCI DSS. The agency will advise OSC, and keep OSC updated with, the name of the agency's PCI contact. This individual is normally the IT Director.

To assist in validating the agency's compliance with the PCI DSS, the agency has enrolled with Coalfire, OSC's selected vendor for providing PCI Security Validation Services. Enrollment is at the "chain level" and provides for: 1) an annual Self Assessment Questionnaire (SAQ) to be completed online; and 2) vulnerability scans required for all capture solutions having external-facing IP addresses (URLs and PC capture software). Scans (do / do not) apply to the agency's applications, and all applicable IP addresses have been enrolled with Coalfire to be scanned monthly. The completion of the annual Self Assessment Questionnaire (SAQ) will be performed each May via Coalfire's Navis Portal, and will be the responsibility of the IT Director. The agency's "chain number" assigned by STMS is 419950034993.

The agency's chain number is enrolled in Coalfire for SAQ and Vulnerability Scanning.
Reference is made to "Policy for PCI Data Security Standards." http://www.osc.nc.gov/SECP/Compliance_with_PCI_Data_Security_Standards.pdf

There are four versions of the SAQ that is to be completed, depending upon the capture method, and upon whether a third-party service provider is utilized or not. https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#instructions. A separate SAQ is to be completed by each division (paper form, not online). Each division may qualify for a different version of the SAQ. Through Coalfire, there should only be one SAQ completed online, the version that is the most stringent. The SAQ to be completed by the agency through Coalfire is (C, or D).

The following merchant numbers are associated with the agency's capture solutions having external facing IP addresses (URLs or POS Capture software) that require monthly vulnerability scans, and are enrolled with Coalfire for the purpose of receiving scheduled monthly scanning: (Identify each merchant account application) Pertinent merchants accounts applications are BIS, Sturgis, networked POS.

In accordance with Section 11.3 of the PCI DSS, applications involving external IP addresses, which store cardholder data, also require "penetration tests" (Network-layer and Application-layer) at least annually, which is different than the vulnerability scanning. Such penetration test will be performed by Coalfire or alternative penetration test provider, and during the month of May. (If cardholder data is not stored on the application, penetration testing is not required.)
https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

The third-party capture applications, BIS and Sturgis must be and remain compliant with the PCI PA-DSS. It must be listed on Visa's CISP website or on the PCI Security Council's website as a "Validated Payment Application." Default passwords are not used. The software is updated within 30 days of the release of any security patches. (Indicate application name and version.)

The following merchant numbers do not require vulnerability scanning, as they do not involve external-facing IP addresses: (Identify each merchant account application): N\A (unless strictly reliant on phone).

In accordance with Requirement 12.8, the third-party gateway vendor, functioning as a "service provider," BIS and Sturgis, must be and remain PCI DSS compliant. A "written agreement" must be in place with the vendor that specifies the vendor's PCI data security responsibilities. The written agreement language is contained in original contract. The agency must monitor the vendor's compliance on an ongoing basis. Evidence of compliance will be obtained from the gateway service provider every year. Refer to the OSC document for reference regarding "PCI Validation for Service Providers." http://www.osc.nc.gov/programs/PCIValidationforServiceProviders.pdf

Issues detected by either the Self Assessment Questionnaires (SAQ), or by Coalfire's vulnerability scans, or by failure of the service provider to demonstrate compliance, will be brought to the attention of the Macon County Finance Director and the IT Director. A plan for remediation will immediately be developed for each incident of non-compliance detected, and the Office of the State Controller will be advised.

Either this policy or separate agency policies address the twelve primary requirements of the PCI DSS, which are categorized in the following areas:

- Build and maintain a secure network (1-2)
  - Install and maintain a firewall configuration to protect cardholder data
  - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data (3-4)
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data and sensitive information across public networks
- Maintain a vulnerability management program (5-6)
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications
- Implement strong access control measures (7-9)
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly monitor and test networks (10-11)
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes (Note 11.3 requires annual penetration tests, which is different than the vulnerability scanning requirement)
- Maintain an information security policy (12)
  - Maintain a policy that address information security
- Compensating Controls

2) System security requirements for merchant card services. Agency will incorporate the following requirements into its processing of merchant cards.

System Settings

- Change vendor default security settings prior to installing the system on the network.
- Disable or change default accounts and passwords prior to installing the system on the network.
- Harden production systems by removing all unnecessary services and protocols.
- Use secure, encrypted communications for remote administrative access.

Stored Data Protection

- Dispose of sensitive cardholder data when it is no longer needed.
- Do not store the full contents of any track from the magnetic stripe in any manner.
- Do not store the card-validation code (the three digit value printed on the signature panel of a card) in any manner.
- Mask all but the last four digits of the account number when displaying cardholder data.
- Accounts numbers must be securely stored by means of encryption or truncation.
- Account numbers must be sanitized before being logged in the audit trail.

- Access to card account numbers must be restricted for users on a need-to-know basis.
- Employees having access to systems containing bulk merchant card data are screened. (12.7) Criminal background checks are performed upon hire.

Transmitted Data Protection

- Transmissions of sensitive cardholder data must be encrypted through the use of SSL.
- Credit card numbers must not be transmitted via email.

Anti-Virus Protection

- All Microsoft Windows Servers and workstations must have antivirus software installed and the virus definitions must be updated regularly.
- Centrally managed Kaspersky Enterprise Antivirus is installed on all workstations. Virus definitions and antivirus status are motored and updated daily.

Applications and Systems Security

- All networks will be established in accordance with the firewall configurations as specified by requirement number 1 of the PCI DSS.
- All systems must be updated with the latest security patches within 30 days of their release.
- The software and development process must be based on industry best practice and information security must be included throughout the process.
- Sensitive cardholder data must be sanitized before it is used for testing and development.
- All changes must be formally authorized, planned and logged.
- Sensitive cardholder data stored in cookies must be secured or encrypted.

Account Security

- All users must authenticate using a unique user ID and password.
- Remote access must be via a secure connection.
- All passwords must be encrypted.
- All user accounts must be revoked immediately upon termination.
- All user accounts must be regularly reviewed to ensure that malicious, out-of-date and unknown accounts do not exist.
- All inactive accounts must be automatically disabled after a pre-defined period.
- Vendor accounts used for remote maintenance must be disabled when not needed
- Group, shared or generic accounts are prohibited.
- Passwords must be changed at least every 90 days; current standards are every 42 days.
- Passwords must follow strong password conventions.
- Multiple password attempts or brute force attacks must result in an account lockout.

Physical Access

- Multiple physical security controls must prevent unauthorized access to the facility.
- Equipment and media containing cardholder data must be physically protected against unauthorized access.
- Cardholder data printed on paper or received by fax must be protected against unauthorized access.
- Proper procedures for the distribution and disposal of any media containing cardholder data must be followed.
- All media devices that store cardholder data must be inventoried and properly secured. The merchant copy of receipts shall be kept for a minimum of 18 months. (Retention should be included in agency's official records retention schedule.)

- Cardholder data must be deleted or destroyed before it is physically disposed (e.g. by shredding paper and degaussing media).
- All cache containing merchant card data must be cleared daily.

Access tracking

- All access to cardholder data must be logged.
- Logs must contain successful and unsuccessful login attempts and all access to the audit logs.
- Critical system clocks must be synchronized with the agency's time server, and logs must include date and time stamps.
- Logs must be secured, regularly backed up and retained for 3 months online and one year offline.

Security breaches – Incident Plan

Agency shall adhere to all requirements pertaining to the establishment of a security incident plan as required* by the PCI Data Security Standard and other applicable policies. This includes any actions necessary to secure any exposed data, to report the incident to appropriate agency management, to report the incident to the Office of the State Controller, and adhering to applicable statues, including the NC Identity Theft Protection Act.

Reference is made to OSC's E-Commerce Policy entitled, "Merchant Cards Security Incident Plan." http://www.osc.nc.gov/SECP/MerchantCardsSecurityIncidentPlan.pdf

H. Training

As specified by requirement number 12 of the PCI DSS, all employees having access to merchant card data must be advised of the expectation of being aware of the sensitivity of data and their responsibilities for protecting it. Each division within the agency acting as a merchant shall ensure that all employees responsible for systems or procedures related to merchant card transactions or data will be provided proper training relating to the policies and procedures for merchant card processing, including being provided a copy of this policy document. Each employee will be required to acknowledge in writing that they have read and understood the agency's applicable security policies and procedures. Additionally, all employees will be advised to refer to the Website on a frequent basis to ascertain any changes or advisements. Most resources can be found on the State Controller's SECP Website: http://www.osc.nc.gov/SECP/index.html

Required resources for training will include:

- SunTrust Merchant Services Operating Guide
- Visa Rules for Merchants
- MasterCard Rules for Merchants
- PCI Data Security Standard
- Other resource materials on the State Controller's SECP Website

The IT Director is responsible for yearly distribution of training materials and resources. Department heads are responsible for documenting acknowledgements of employees training and policy acceptance. Signed acknowledgements are to be filed with the HR Department. HR will provide the training and policy materials to new employees as applicable.

I. Business Functions

1) Authorizations

- Reference is made to OSC's E-Commerce Policy entitled, "Authorization for Merchant Card Transactions." http://www.osc.nc.gov/Credit_Card/AuthorizationforMerchantCardTransactions.pdf
- Reference is also made to SunTrust Merchant Services Operating Guide. http://www.osc.nc.gov/SECP/OperatingGuide-OPSG801_.pdf
- For face-to-face transactions, the card holder's signature must be verified.
- For card not-present transactions, (specify if Secure Code or Address Verification will be used)
- Prior to the finalization of a merchant card transaction, an authorization approval code must be obtained from the merchant card processor (depends upon capture method being used).
- Real-time authorization shall be the preferred method, with the telephone authorization being the alternative method.
- If no authorization is received, card cannot be accepted and an alternative means of payment will be requested.
- If a suspected fraud is detected (code 10 authorization), procedures as outlined in SunTrust Merchant Services Operating Guide will be followed.

2) Refunds / Credits

- Reference is made to procedures prescribed in the SunTrust Merchant Services Operating Guide. http://www.osc.nc.gov/SECP/OperatingGuide-OPSG801_.pdf
- No cash refunds shall be given
- Refunds are to be made in the exact dollar amount as the original transaction, and to the same card originally used

3) Fulfillment and Shipping of Goods

- Reference is made to procedures prescribed in the SunTrust Merchant Services Operating Guide. http://www.osc.nc.gov/SECP/OperatingGuide-OPSG801_.pdf

4) Cut-off Times and Close Outs

- The following cutoff times are established for POS terminal transactions: 5:00pm, unless business unit office hours proceed that.
- The following cutoff times are established for Internet transactions: N\A
- Close out and transmissions of data may be real time, or outside of normal business hours.

J. Fiscal Office Functions

1) Reconciliation

- Reference is made to the guidelines specified on the State Controller's SECP Website: http://www.osc.nc.gov/SECP/SECP_MerchantCard_Reconciliation.html
- The following tools shall be utilized in the process:2) Wells Fargo CEO;
- The following reports will be used in the reconciliation process: Previous Day Composite Report and Settlement Report
- All deposits shall be reported through CMCS in accordance with established procedures, as "type 4." On a daily bases.
- The Finance office will be responsible for ensuring that all necessary reconciliations are performed.
- Bank account statements received for the settlement account will be reconciled by The Finance Department.

- In the case of multiple merchant numbers established for decentralized agency divisions. Finance department reconciles all merchants' numbers.

2) Chargebacks

- Reference is made to OSC's E-Commerce Policy entitled, "Customer Transaction Disputes." http://www.osc.nc.gov/Credit_Card/CustomerTransactionDisputes.pdf
- Reference is made to procedures prescribed in the SunTrust Merchant Services Operating Guide. http://www.osc.nc.gov/SECP/OperatingGuide-OPSG801_.pdf
- Copies of transaction slips and other documentation will be kept for a minimum or 18 months, and in accordance with agency official records retention schedule, in each department.
- Requests from STMS for copies of transactions shall be supplied within the timeframe set forth in the notification.
- Agency will act in good faith in resolving any disputes received from cardholders.
- Chargebacks that are debited against the settlement bank account treated like returned checks.

3) Paying Invoices

- All invoices for services received (e.g., SunTrust Merchant Services, external vendor, etc) shall be paid timely, in accordance with established agency procedures for accounts payable.
- On a periodical basis, the interchange rates shall be inspected to ensure that the best rates are being obtained.
- Responsibility for inspecting the invoices received and approving for payment is that of the Finance office.

II. EXHIBITS AND SUPPLEMENTAL PROCEDURES

A. Office of the State Controller (OSC) Policies

Electronic Commerce Policies issued by the State Controller are incorporated herein. The policies are located on the OSC Website at the following address:
[http://www.osc.nc.gov/SECP/SECP_Policies.html]

B. Other Applicable Policies

Reference other policies that may be applicable.

C. Supplemental Procedures

Acknowledgment

I have received a copy of Internal Policies and Procedures for Merchant Card Processing and I have read and understand the policy. I agree to observe the terms and conditions of this policy.

Signed Name:________________________________

Printed Name:________________________________

Date: ____________________