

Policy and Guidelines For Electronic Commerce

| | | |
|---|---|---------------------------------|
| Office of the State Controller (OSC) | | Effective Date: October 1, 2008 |
| Policy Area: Electronic Commerce | Title: Compliance with PCI Data Security Standards | |

Authority: Session Law 1999-434, Senate Bill 222, ratified in July 1999 amended various statutes, authorizing state government agencies to maximize the acceptance of electronic payments, a term which includes credit / debit cards (merchant cards) and electronic fund transfer (EFT). Electronic payments involve both inbound and outbound flows of funds. The primary statutes pertaining to the utilization of electronic payments for State agencies include: G.S. 147-86.10; G.S. 147-86.11(h); G.S. 147-86.20; G.S. 147-86.22; and G.S. 143B-426.40G(a).

Statutes authorizing the Office of the State Controller to issue policies regarding electronic payments include G.S. 143B-426.39(1) and (5); G.S. 147-86.11(a); and G.S. 147-86.22(b).

“Electronic Commerce in Government” is covered under Chapter 66, Article 11A (G.S. 66-58.1 through 66-58.19). G.S. 66-58.12 encourages the utilization of electronic transactions, including those initiated through the Internet, and requires consideration of security and privacy issues. Other applicable statutes include G.S. 132 (Public Records Law) and G.S. 14-113.24 pertaining to credit card numbers. Local units of government are eligible to participate in master agreements administered by the State pursuant to G.S. 147-33.82(b).

Program Administration: The Office of the State Controller (OSC) provides eligible entities (including state agencies, universities, community colleges, and local units of government) the opportunity to secure merchant card services under a master services agreement.

Statutory Requirements: G.S. 66-58.12(a) states in part, “Public agencies...shall identify any inhibitors to electronic transactions between the agency and the public, including legal, policy, financial, or privacy concerns and specific inhibitors unique to the agency or type of transaction. An agency shall not provide a transaction through the Internet that is impractical, unreasonable, or not permitted by laws pertaining to privacy or security.”

G.S. 132-6.1(c) states in part, “Nothing in this section requires a public agency to disclose security features of its electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes.”

G.S. 147-33.82(b) states, “Notwithstanding any other provision of law, local governmental entities may use the information technology programs, services, or contracts offered by the Office, including information technology procurement, in accordance with the statutes, policies, and rules of the Office.”

Reference: The Office of the State Controller’s policy entitled, “Security and Privacy of Data,” which should be considered when construing this policy, contains two policy requirements that state:

- All participants in any of the Master Services Agreements (i.e., Merchant Card Services and Electronic Funds Transfer Financial Services), as well as State agencies engaging in separate

arrangements, are to adhere to the appropriate security and privacy requirements that may govern the entity.

- In the case of Merchant Card services, each participant must...participate in any security assessments and security scans required by the associations and/or OSC, in order to be and to remain compliant with Payment Card Industry (PCI) Security Standards, and be responsible for any fines levied as the result of not being compliant.

Additionally, the Master Services Agreement with the merchant card vendor states, “The vendor and participant shall comply with all Payment Card Industry (PCI) security standards.”

The PCI Data Security Standards are those issued by the PCI Security Standards Council, which may be viewed at the Council’s website: <https://www.pcisecuritystandards.org/>

Policy: Notwithstanding any conflict with the referenced “Security and Privacy of Data Policy” or with the Master Services Agreement with the merchant card vendor, the following requirements are to be adhered to:

- For all participants in the Merchant Card Services master agreement provided by Office of the State Controller (OSC), the OSC shall secure the services of a security services provider considered to be both a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV), for the purposes of providing both remote validation services and vulnerability scanning services. Costs of the various services secured from the security services provider may be borne by either the OSC and/or the participants as may be determined appropriate by the OSC.
- As a prerequisite for participating in the master services agreement, each participant must enroll in the services provided by the security services provider:
 - All participants must subscribe to the service that provides for the annual completion of the appropriate online Security Assessment Questionnaire (SAQ), as required by the PCI Data Security Standard.
 - All participants that utilize one or more capture methods involving external facing IP addresses, and are subject to undergoing vulnerability scans as required by the PCI Data Security Standard, are to subscribe to the vulnerability scanning service.
- Any costs incurred by a participant to become and remain compliant with the PCI Data Security Standards, including but not limited to an annual penetration test (if applicable), shall be borne by the participant. Any costs incurred by the participant associated with an onsite security audit or a forensic investigation that may be required shall be borne by the participant.
- Any participant that does not enroll or remain enrolled in the validation service provided by the securities services provider shall not be allowed to participate or continue its participation in the Merchant Card Services master agreement.
- Each participant enrolled in the validation service provided by the security services provider shall perform all requirements of the service in a timely manner in order to reflect and attest the status of compliance with the PCI Data Security Standard.
- The Office of the State Controller shall periodically compile reports obtained through the validation service reflecting and attesting the status of compliance with the PCI Data Security Standard (PCI DSS). The reports shall be made available to the merchant card processor, as may be requested from time to time by the processor, or as may be requested by a card brand. The information provided

shall only be to assist the participants in attesting their compliance with the PCI DSS, as may be required by the master services agreement(s).

- In the case where the participant is subject to the oversight of a central oversight agency, the Office of the State Controller may share the compliance status reports obtained through the validation service with the appropriate central oversight agency. Appropriate management reports may be submitted as follows:
 - State Agencies – Office of Information Technology Services
 - Universities – UNC General Administration
 - Community Colleges – NC Community College System
 - Local Units of Government – Local Government Commission
- When appropriate, and/or when requested, the management reports shall be submitted to the Office of the State Auditor.
- The role of the Office of the State Controller shall not be to make determination if a participant is compliant with the PCI Data Security Standard or not, but to provide information that may be obtained through the validation service to the merchant card processor (vendor). The merchant card processor will use the information provided to determine the participant's compliance status and to determine any rectifying action that the processor deems appropriate to address any non-compliance issue. The processor may address any non-compliance issue directly with the participant.
- Pursuant to G.S. 132-6.1(c), the information obtained through the validation service regarding a participant's PCI Data Security compliance status shall be deemed confidential, as the information would disclose security features of the participant's electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems. Accordingly, any reports shared with the central oversight agencies are to be treated as confidential information pursuant to the referenced statute.
- Any participant receiving communications from the merchant card processor regarding a PCI Data Security non-compliance issue must respond to the processor within a reasonable time. Corrective actions must be taken that satisfies the processor's concerns. Actions taken may include, but not be limited to:
 - Correcting the non-compliance issue within the timeframe agreed to by the processor
 - Implementing compensating measures agreed to by the processor
 - Temporarily suspending the use of a merchant card capture application until the non-compliance issue is resolved
 - Discontinuing the merchant card capture application altogether
- In the case of a communication received from the merchant card processor regarding a PCI Data Security non-compliance issue, where the participant is subject to the purview of a central oversight agency (i.e., Office of Information Technology Services, UNC-General Administration, NC Community College System, Local Government Commission), guidance from the central oversight agency should be sought by the participant.
- For State agencies operating a merchant card capture system, but not participating in a master services agreement provided by the Office of the State Controller (OSC), the agency may apply to enroll in the validation service offered by OSC for PCI Data Security compliance purposes. However, community colleges that are not participants in a master services agreement provided by

OSC are to enroll in a validation service offered by the NC Community College System, and are subject to the requirements of the college's contracted merchant card processor.

- The individual (or his/her successor) at the governmental entity that executed the "Participation Agreement" to allow the entity to be a participant in OSC's merchant card services master services agreement shall be the individual responsible for ensuring that the requirements of this policy are adhered to, including but not limited to, responding to any non-compliance issues that may arise.