

2011 PCI DSS Certification Letter

State Treasurer Stenberg:

I certify that my agency has met the PCI Data Security Compliance Standards as required by the Card Associations (Visa, MasterCard, American Express and Discover).

I have attached the PCI Data Security Standard SAQ D and Attestation of Compliance Version 1.2 audit report for review by the Treasurer's Office and CIO staff. Our agency has carefully, thoroughly, and truthfully completed a full audit as required, scans (if required), and our agency has disclosed any or all PCI concerns/compliance issues. Our agency has also reviewed our security procedures and policies that pertain to PCI Compliance.

I certify that all scans have been performed by a Qualified Security Assessor PCI Scanning Vendor and I have verified that the scanning entity's name is on the Visa and MasterCard Association list of approved vendors. (Only applies to agencies that are required to submit quarterly scans).

I certify that all forms and merchant slips received by our agency that contain credit card data are stored in a locked/secured cabinet with limited access to key staff as needed. The locked cabinet is secured at all times, and access is granted only to authorized state agency personnel. **A staff member from my agency participated in one of the 2011 PCI DSS training opportunities (either the conference call or in-person meeting).**

I certify that our computer servers, switches, and equipment storing credit card data are located in a secured area/room within our agency that has limited access to authorized agency personnel only.

I certify, if our agency outsources credit card processing to a third party vendor, the vendor is compliant with PCI DSS requirements. I understand it is my responsibility to verify that this compliance remains current during the term of services with the third party vendor. I understand that the following two paragraphs also apply if my agency has hired the third party vendor for credit card services.

I understand that if I have a security breach or compromise of data, I am required to immediately disclose this information to the State Credit Card Merchant Bank, the State Treasurer's Office, the Office of the CIO, the FBI, the Nebraska State Patrol and other law enforcement (as directed by the CIO's and Treasurer's Offices). I understand that if I fail to immediately report a breach or data compromise I will be responsible for the additional Card Association fines.

I understand that our agency is financially liable for any cardholder data compromised including but not limited to: any fines/penalties or punitive damages charged by the Card Associations; costs (if charged) incurred by law enforcement; reimbursement costs/expenses (if charged) by the Card Associations; expenses/costs (if charged) by the State of Nebraska CIO's Office; expenses/costs (if charged) by the State Treasurer's Office; and fees/costs of the company hired to complete the forensic scan and assist in the investigation. I understand that any and all additional costs incurred due to a breach of any type will be the responsibility of my office.

The following list of forms are required to be turned into the Treasurer's Office no later than June 6, 2011:

1. PCI Data Security Standard SAQ D and Attestation of Compliance V 1.2 (either Word or PDF version)
2. 2011 PCI DSS Certification Letter
3. 2011 PCI DSS agency information sheet

\_\_\_\_\_  
Printed Name – Agency Director

\_\_\_\_\_  
Printed Agency Name

\_\_\_\_\_  
Signature - Agency Director

\_\_\_\_\_  
Date