STATE OF NEW MEXICO
PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS
GUIDANCE ON – CONTRACT CLAUSES SUPPORTING VENDOR MANAGEMENT PROGRAM

Outsourcing of payment card activities is an effective means of reducing PCI-DSS scope. However, outsourcing does not relieve the Agency from ensuring cardholder data is secured. To assure our service provider protects cardholder data requires development and implementation of a vendor management program. With that objective in mind, contracts should include appropriate language to hold vendor responsible for protection of card data to which they have access or process.

Depending on the activities outsourced, the following clauses or clauses similar to the following should be considered for inclusion in your contracts.

PCI DSS Compliance Clause

The State of New Mexico is required to periodically demonstrate compliance with PCI DSS (Payment Card Industry Data Security Standard). The compliance process requires the STATE to undergo an assessment that includes all the system components used to process, store or transmit cardholder data, and any other component that resides on the same network segment that those system components, hereafter known as "System Components in Scope". Some of those system components and/or processes have been outsourced to SERVICE PROVIDER.

SERVICE PROVIDER will achieve and maintain PCI DSS compliance against the current version of PCI DSS published on the PCI SSC (PCI Security Standards Council) website. As evidence of compliance, SERVICE PROVIDER will provide when requested, a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor) If SERVICE PROVIDER is unable to provide a current attestation of compliance, SERVICE PROVIDER will allow the STATE'S QSA to assess all the system components in scope that are hosted or managed by SERVICE PROVIDER, and the related processes used to process, transmit or store cardholder data.

SERVICE PROVIDER will create and maintain reasonable detailed, complete and accurate documentation describing the systems, processes, network segments, security controls, and dataflow used to receive, transmit, store and secure the STATE'S cardholder data. Such documentation will conform to the most current version of PCI DSS. SERVICE PROVIDER will, upon written request by the STATE, make such documentation and the individuals responsible for implementing, maintaining and monitoring those system components and processes available to:

a) QSAs, forensic investigators, consultants or attorneys retained by the STATE to facilitate audit and review of the STATE'S PCI DSS compliance.
b) STATE'S IT Staff.

[SERVICE PROVIDER} will retain such documentation until ____ years after termination of this agreement.

Security Clause

SERVICE PROVIDER will use reasonable precautions, including but not limited to, physical, software, and network security measures, employee screening, training, and supervision and appropriate agreements with employees, to prevent anyone other than STATE or its authorized employees from monitoring, using, gaining access to or learning the import of STATE Data; protect appropriate copies of STATE Data from loss, corruption or unauthorized alteration; and prevent the disclosure of STATE passwords and other access control information to anyone other than authorized STATE employees.

SERVICE PROVIDER will periodically test and re-evaluate the effectiveness of such precautions. SERVICE PROVIDER will notify the STATE within ____ hours, if such precautions are violated and STATE Data are affected thereby or passwords or other access information is disclosed. Notwithstanding the foregoing, SERVICE PROVIDER and its employees may use, process, view the contents of or monitor STATE Data to the extent necessary for SERVICE PROVIDER to perform under this agreement.

Data Retention Clause

SERVICE PROVIDER will erase or destroy all media under its control containing copies of STATE Data not later than ____ days after the processing of such data, except where special circumstances, of which SERVICE PROVIDER has given The STATE written notice, warrant longer retention. For purposes of this agreement, to "erase" means to render the relevant data unrecoverable by any means according to PCI DSS Requirement v.9.8.2.

Data Ownership Clause

SERVICE PROVIDER has no property interest in, and may assert no lien on or right to withhold from the STATE, any data it receives from, receives address too, or stores on behalf of the STATE.

Archive Segregation Clause

All records, data and files stored by the [SERVICE PROVIDER] as archives of STATE Data including the media on which they are stored, are the exclusively property of STATE, and SERVICE PROVIDER may assert no lien on or right to any of the same. SERVICE PROVIDER will conspicuously mark all such archival storage media as STATE property. At STATE'S request, SERVICE PROVIDER will, for [a certain fee], promptly deliver to STATE and if requested destroy any other remaining copies that the STATE will no longer need.

Subpoena Clause

If SERVICE PROVIDER is served with a warrant, subpoena or any other order or request from a government body or any other person for any record or files of STATE Data, SERVICE PROVIDER will, as soon as reasonably practical and not in violation of law, deliver to STATE a copy of such warrant, subpoena, order or request and will not, without STATE's prior written consent, comply with the same unless and until required to do so under applicable law.

PCI DSS Clause for Software Vendors

Software Vendor warrants that the Software meets PA-DSS (Payment Application Data Security Standard) requirements, and that the STATE following Vendor's instructions detailed in the PA-DSS Implementation Guide will be able to deploy and maintain the Software according to PCI DSS (Payment Card Industry Data Security Standard) requirements. Vendor agrees to indemnify and hold the STATE harmless from any claims, damages, and cause of action, costs and expenses arising out of or related to any breach of the warranty set forth in this paragraph. In the event that security vulnerabilities are identified on the Vendor's Software, VENDOR will promptly notify the STATE and will provide instructions to mitigate risk of that vulnerability being exploited. VENDOR will provide a patch release or security update within ___ days of a security vulnerability being discovered, and will provide support as necessary to properly deployed the patch or security update.