STATE OF NEW MEXICO
PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS
POINT OF SALE RECOMMENDED PRACTICES

Agencies using a payment card processing procedure that employs Point of Sale (POS) card readers, should ensure that the following five activities be in place to protect the state and our clients from POS device tampering.

Inventory

- Maintain a list of the POS terminals and card readers by location. This would include the following essential data: the type, make, model and serial number.

Inspect

- Familiarize yourself with the appearance and location of each POS device and the related connecting cables.
- Each POS device should be checked daily and verified back to the list.
- Check that serial numbers on the terminals match the serial numbers displayed on the terminal screen and equipment list.
- Check for signs of terminal and component tampering; and making sure that staff using these machines are trained to identify evidence of physical tampering.
- Checking that stickers and other visual identifiers are unchanged.
- Prohibit unauthorized personnel from accessing terminals.
- A best practice is to periodically photograph each POS device in inventory and compare the latest images to the "known good" reference images to detect differences that may be potential indicators of compromise.

Secure

- At the end of each business day the POS custodian should secure each POS device. Mobile devices should be secured out of sight and in a locked check-out desk or locker.
- Unless the device is a mobile unit, POS should be secured to registers, desks, etc. so that they can’t easily be physically removed from the premise.

Reporting

- If a POS is stolen, report it. Also you need to be certain that no card holder data is stored on it.
- Notify the agency PCI contact or CFO immediately if anything unusual occurs, such as a sudden change in appear of new connections.

Document

- Maintain documentation showing the status of each device in inventory along with its inspection history. These reports provide proof for internal or external auditors that inspection is occurring according to policy