

# State of Texas - CJIS Security Policy

The Texas Department of Public Safety (DPS) embraces the FBI CJIS Security Policy (CSP) as the security policy for the State of Texas.

Consistent with and in addition to the CSP, DPS requires each agency to adhere to the following rules. These are recognized computer security best practices and these additional rules shall be followed by all agencies that access Criminal Justice data in the State of Texas.

## 1. System Updates

All components of IT systems with CJIS connectivity shall be updated with all available Security Hot fixes, Updates and Patches within 30 days of availability. This applies to workstations, servers, laptops, switches, routers, and all other managed IT equipment.

## 2. End of Life Equipment

All IT systems with CJIS connectivity shall be replaced within 6 months of becoming "end of life", or no longer supported by the manufacturer with Security Hot fixes, Updates and Patches.

## 3. Physically Secure Location

A physically secure location is a facility, an **enclosed** police vehicle, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

## 4. Compensating Controls for Advanced Authentication

### Compensating Controls for Advanced Authentication for Smartphones or Tablets

The APB has passed a Compensating Controls for Advanced Authentication policy for use with Agency issued and controlled Smartphone or Tablets. The compensating controls may be used under these very specific conditions in lieu of Advanced Authentication for these types of devices in the State of Texas.

The Texas CSO has put in place the following process for approval of the compensating controls in the policy:

- The Smartphone or Tablet must be Agency owned.
- Mobile Device Management software must be implemented to control these devices.
- A minimum of four of the listed examples in the policy must be implemented.
- An email must be sent to [securitycommittee@dps.texas.gov](mailto:securitycommittee@dps.texas.gov), requesting conditional approval of the compensating controls.
  - The "Subject line" should read - Request for AA Compensating Control Approval.
  - The body should include your Agency name and contact information and a list of implemented controls from the policy.
- The email should be kept and will be a required item at the agency's next on-site technical audit.

If the above process is completed, it will result in conditional approval of your compensating controls for Advanced Authentication until the Technical Audit team can arrive on-site to perform an audit of the agency's implementation. After approval, you may proceed with a Smartphone or tablet implementation at the agency.

## Policy Statement – Texas CJ Storage Providers

Revised 08/18/2014

The Texas Department of Public Safety (DPS), as CJIS Systems Agency (CSA) for the state of Texas, has modified the rules associated with the adjudication of criminal history background checks associated with entities that contract with criminal justice agencies to perform certain aspects of the administration of criminal justice. The specific area of policy change addresses those vendors that provide offsite storage of hard-copy CJ or CJ document destruction as a result of a contract with a criminal justice agency that is subject to a CJIS Security Addendum.

The vendor employees that have this specific hard-copy only access will be held to the standards articulated within the CJIS Security Policy, but will be allowed access to this hard-copy CJ as long as **a felony conviction** of any kind does not exist on the vendor employee's national finger print based record check processed as part of the requirements of the Security Addendum.

The CJIS Security Addendum must be executed with the vendor company and each employee with hard copy access to CJ must sign a Certification page. All other aspects of the CJIS Security Policy must be followed.

Because vendors for this type of service cannot effectuate changes to the source of the CJ, DPS will lessen the CHRI adjudication standard for this group only. Others in the vendor community that support IT efforts, network support, or are under Management Control still must meet the adjudication standard as currently defined by TCOLE.