**Criminal Justice Information (CJI) Access Management Policy**

**Purpose:**  
This policy establishes guidelines for granting, maintaining, and revoking access to Criminal Justice Information (CJI) in accordance with the Criminal Justice Information Services (CJIS) Security Policy. It ensures secure and controlled access to CJI while maintaining compliance with applicable laws and regulations.

**Scope:**  
This policy applies to all employees, contractors, and personnel requiring access to CJI within the **[Agency Name]**.

**1. New Hire CJI Access Procedures**  
Upon completion of fingerprinting, fingerprint-based background checks, and administrative hiring paperwork, Professional Standards will request CJI access for applicable new employees.

1.1 **Security Awareness Training:**

* All employees must complete Security Awareness Training within six (6) months of being hired.
* Employees must retake Security Awareness Training every twelve (12) months thereafter.

1.2 **Point of Contact for CJI Access Requests:**  
The designated point of contact for CJI user creation, activation, and removal is **[Insert Agency-Designated Role or Office]**. **[Agency Name]** shall assign a responsible individual or office to handle the following duties:

* Notifies relevant personnel of a new employee's hire date and status.
* Submits a request to Information Technology (IT) for access to CJI programs, including but not limited to:
  + Records Management System (RMS)
  + Computer-Aided Dispatch (CAD)
* Creates a new user account in CJIS Online.
* Completes a TLETS User Request Form (URF) and submits it to the Texas Department of Public Safety (DPS) at **TLETS@dps.texas.gov**, as required based on the position and training requirements.

**2. CJI User Account Deactivation and Removal**  
When an employee’s status changes (e.g., resignation, termination, role change), their access to CJI must be promptly revoked.

2.1 **Point of Contact for CJI Access Removal:**  
The designated point of contact for disabling or removing CJI users is **[Insert Agency-Designated Role or Office]**. **[Agency Name]** shall assign a responsible individual or office to handle the following duties:

* Notifies relevant personnel of the employee’s status change and effective date.
* Submits a request to IT for removal of CJI program access, including but not limited to:
  + RMS (Records Management System)
  + CAD (Computer-Aided Dispatch)
* Deactivates the user account in CJIS Online.
* Disables the user in OpenFox.

**3. Compliance & Audit**

* All accounts shall be reviewed at least annually by the designated CJIS point of contact (POC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The POC may also conduct periodic reviews.
* Any discrepancies or unauthorized access must be reported immediately to the designated security personnel.
* Non-compliance with CJIS Security Policy may result in disciplinary action, including termination and legal consequences.

**4. Policy Review & Updates**

* This policy will be reviewed annually or as necessary to ensure continued compliance with CJIS Security Policy.
* Updates to this policy will be communicated to all relevant personnel in a timely manner.

**Effective Date:** **[Insert Date]**  
**Authorized by:** **[Name & Title]**  
**Agency Name:** **[Insert Agency Name]**