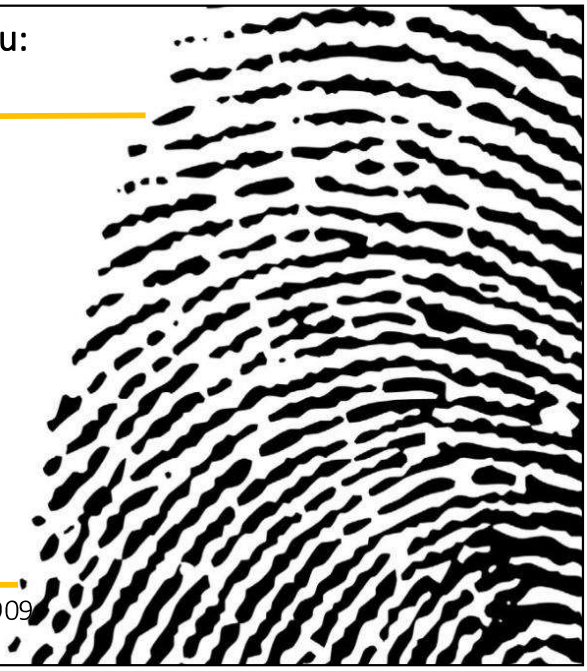
# Compliance & Training Bureau: Secure Site NB/FP Training



Crime Records Division

Audit & Training Unit

Ph: 512-424-2474, option 3 Fax: 512-424-2909

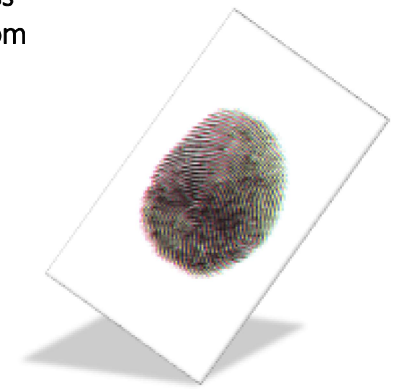
# Table of Contents


- Secure Site Units
- Laws and Policies
- Access to CHRI
- Required Training
- Security and Storage
- Sanitization and Destruction
- Outsourcing
- Secure Site
  - Account Management
  - Name-Based Searches
  - FACT Clearinghouse
  - Clearinghouse Worklist
  - Applicant Detail Page
  - Subscribing and Unsubscribing
  - Clearinghouse Subscription list
  - Clearinghouse Fingerprints Rejection Message
  - Clearinghouse Notifications
  - Clearinghouse Search History
  - Rap Back Program
  - Secure Site Fees
- Audits
- CJIS Launch Pad
- Crime Records Link
- Contact List

## Secure Site Units

All units work together to provide agencies access to Criminal History Record Information (CHRI) from the Secure Site.

- *Access and Dissemination Bureau*
  - Fingerprint Services Unit
  - Criminal History Inquiry Unit
  - Billing Unit
  - ADB Support Unit
- *Compliance and Training Bureau*
  - Non-Criminal Justice Audit and Training Unit



These all the units that would together to make sure we can assist you.

- Fingerprint Services Unit: Helps with fingerprint rejects, problems with the FACT clearinghouse, service codes and FRB status problems.
- Criminal History Inquiry Unit: Open/Closes accounts, adds/removes users, unlocks accounts, helps with legislative authority.
- Billing Unit: Billing issues if your agency gets billed.
- ADB Support Unit: Fingerprinting vendors, locations, complaints, suggestions.

# Laws And Policies

411 Texas Government Code

- GC §411.084 Use of Criminal History Record Information
  - (a-1) The term "criminal history record": The information contained, wholly or partly, in a document's original form or any subsequent form or use.
  - (c) An agency or individual may not confirm the existence or nonexistence of criminal history record information to any person that is not eligible to receive the information.
- GC §411.085 Unauthorized Obtaining, Use, or Disclosure of Criminal History Record Information; Penalty.
  - Class B Misdemeanor
  - Second Degree Felony
- Do you know your 411 Texas Government Code?
  - https://statutes.capitol.texas.gov/

It is very important to know your 411 statue that grants you access to the TX DPS Secure Site, if you do not know your own please contact our email: CJIS.audit@dps.texas.gov

# Laws And Policies

Access and Dissemination Policy – Located on the Secure Site and the CJIS Launch Pad

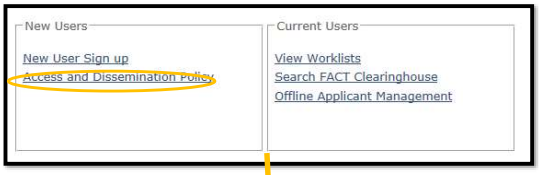
- **Access by Criminal and Non-Criminal Justice Entities**
  - Legislative Authority for Criminal and Non-criminal Justice Entities' Access
  - Agency User Agreements
- **Personnel Security**
  - Authorized Users
  - User Identifier
  - Personnel Sanctions
- **Facility And Information Security**
  - Facility Security Standards
  - Physical Protection
  - Information Security Standards
  - Media Protection
- **Criminal History Record Information**
  - Obtaining, Use and Dissemination of Criminal History Record Information
  - Dissemination is **Restricted**
  - FACT Clearinghouse Subscriptions
    - Unsubscribe to individuals who are no longer associated with the agency within 3 business days.
- **Incident Response Policy**
  - Reporting Security Events
- **Criminal Justice Information Services (CJIS) Security Policy**
  - CSP Version 5.9.2
  - Security Audits

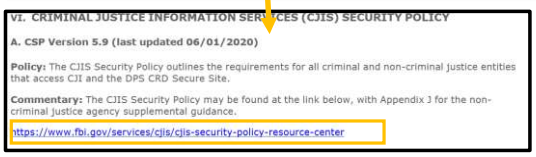
The FBI requires that DPS has security policies that is the Access and Dissemination Policy the FBI also requires you to have policies, these are different policies that your agency should have in place if your are access CHRI. We have a sample in our CJIS launch pad you also have to have an incident reporting form in place. CJIS Launch Pad https://texas.cjisapps.com/noncrim/launchpad/cjisdocs/docs.cgi

# Laws And Policies

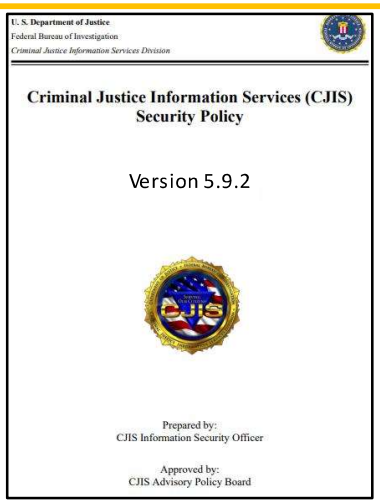
## How to Find the Access and Dissemination Policy and how to Find the Criminal Justice Information Services (CJIS) Security Policy :

- Select Criminal History Search or FACT Clearinghouse
- Select A&D Policy under "New Users"
- Scroll to the bottom of page for CJIS Security Policy and open FBI link.



# Laws And Policies


U. S. Department of Justice
Federal Bureau of Investigation
*Criminal Justice Information Services Division*

**Criminal Justice Information Services (CJIS) Security Policy**

Version 5.9.2

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

CJIS Security Policy

- Is provided by the FBI for all agencies with access to CHRI.
- The Access and Dissemination Policy cites the CJIS Security Policy.
- The FBI along with DPS will audit agencies.

This is the FBI Security policy it outlines the minimum standards for security, anyone who access Fingerprinting (FACT) should be aware of for their future audits. Some of the polices you want to review are for example an Outsourcing Agreement, FIPS 140-2, and CJIS Security Awareness Training. https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center

# Laws And Policies

## CJIS Policies – Sample Policy is Available

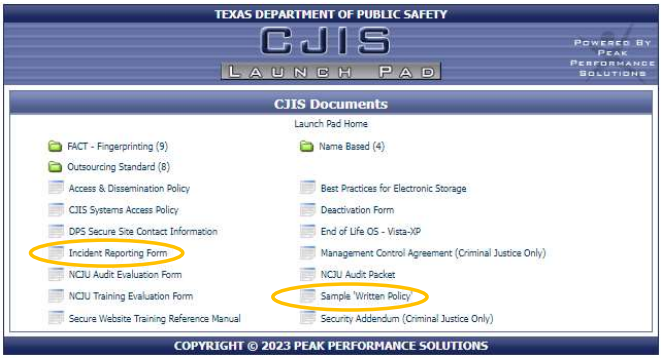
- **Agencies will need to implement the following:**
  - Policy for the discipline of CJIS violators. **(CSP 5.12.4)**
  - Physical protection policy to ensure Criminal Justice Information (CJI) is secured. (Access to secure areas) **(CSP 5.9)**
  - Protection and procedures policy to ensure digital and physical media in all forms is secured. **(CSP 5.8)**
  - Policy and procedures for the sanitization and destruction of electronic media. **(CSP 5.8)**
  - Policy and procedures for the disposal and destruction of physical media. **(CSP 5.8)**
  - Incident response policy. **(CSP 5.3 & 5.13.5)**

If you do not have policies, we have policies in our CJIS launch pad.

# Laws And Policies

## CJIS Policies – **Sample Policy is Available**

- Sample policy and Incident Reporting form both found on CJIS launch pad.



**Agency**
**INCIDENT**
**REPORTING FORM**

DATE OF REPORT (MM//DD/YYYY): _____

DATE OF INCIDENT (MM/DD/YYYY): _____

NAME: _____

PHONE: _____

EMAIL: _____

LOCATION(S) OF INCIDENT: _____

AREA AFFECTED: _____

METHOD OF DETECTION: _____

DESCRIPTION OF INCIDENT (e.g. access, use, retention, dissemination etc.):

ACTIONS TAKEN/RESOLUTION:

**Copy to:**
Attn: Erika Staggers
Crime Records Division
Compliance & Training Bureau
Audit and Training Unit
Texas Department of Public Safety

Email: CJIS.Audit@dps.texas.gov
Fax: 512-424-2909

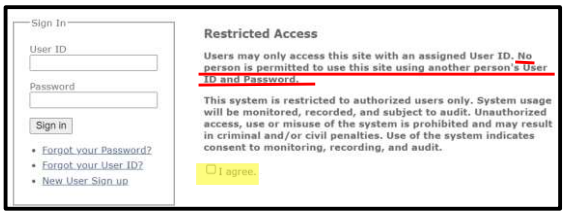
# Access to CHRI

<u>Least Privilege – CJIS Security Policy 5.5.2.1</u>

- The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.
  - The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.
  - This limits access to CJI to only authorized personnel <u>with the need and the right to know.</u>

# Access to CHRI

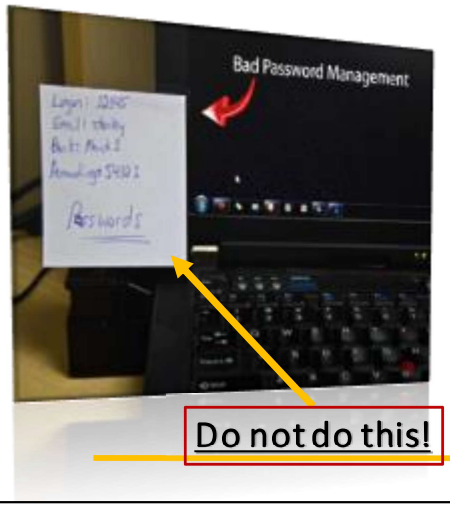
## Access to Physical Media and Digital Media




- Read and select "I agree" for Restricted Access Notification.
- Only individuals who are authorized to view CHRI may have access.
- Individuals who have completed the ***CJIS Security Awareness Training*** are considered authorized. *(FP agencies only)*
- **Do not** share your credentials that grant you access to the Secure Site.

Every time you enter our secure site you are agreeing to not share CHRI with anyone unauthorized and to no share your credentials with anyone.

# Access to CHRI




## Acceptable Password Management

- Notebooks, locked up securely
- Excel spreadsheets with encryption
- Password managers with encryption
- **Do not** auto-save, auto-fill or share passwords.
- Memorized secret verifiers shall not permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.

## Additional compliance items:

- A session lock shall be in place of 30 minutes or less.
- Computer monitors shall be positioned to prevent the unauthorized viewing of CHRI, if this is not possible privacy screen protectors shall be in place.

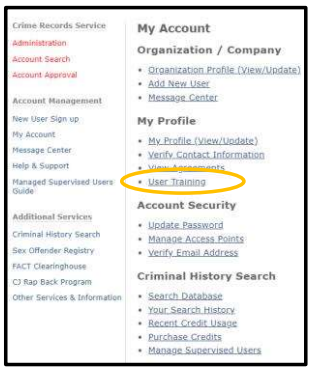
# Access to CHRI

Physical Access to Secured Areas – CJIS SP 5.9

**Secured Area is where the CHRI is retrieved, viewed, and stored**

- Control all physical access points for secured areas
- Authenticate visitors prior to access
- Escort visitors at all times
- Control access for data closet containing the network servers
- Secure print for network printer (password) https://adminit.ucdavis.edu/tech-tips/how-secure-print

# Required Training




| Course Description | Status | |
|---|---|---|
| Criminal History - 1. Introduction and Overview | PASS | Training |
| Criminal History - 2. Account Management | PASS | Training |
| Criminal History - 3. Handling Information | PASS | Training |
| Criminal History - 4. Name-Based Searches | PASS | Training |
| Criminal History - 6. FACT Clearinghouse | PASS | Training |

## Secure Site Training Modules

- All modules must be completed prior to usage of the Secure Site.
- Depending on the status of the user, some will take more modules than others.
- Modules will train the user how to use the Secure Site.
- It is a one-time exam per module unless there is an update. You may review modules at anytime.

# Secure Site

## My Account

Navigation Area

- Select "My Account"

Data Users and Supervisors:

- Must complete training.
- Sign Agreements, if not, data user will be locked out.
- If supervisor does not sign, both will be locked out.

**My Account**

**Organization / Company**

- Organization Profile (View/Update)
- Add New User
- Message Center

**My Profile**

- My Profile (View/Update)
- Verify Contact Information
- View Agreements
- User Training

**Account Security**

- Update Password
- Manage Access Points
- Verify Email Address

**Criminal History Search**

- Search Database
- Your Search History
- Recent Credit Usage
- Purchase Credits
- Manage Supervised Users

Supervisors:
View Data Users for the Organization.
*Ensure everything is current*

Supervisors:
Monitor searches and manage users.

# Secure Site

## Supervisors – Manage Users

- **My Account**
  - Manage Supervised Users
  - Select Display all Accounts
  - Active data users should be "Supervised by me"
  - If data users are not supervised, they will be locked out.
- **Expired Supervisors:**
  - No activity for 90 days will expire users.
  - If supervisor is expired, the whole account will be locked.
  - Contact Criminal History Inquiry Unit at NCJU@dps.texas.gov or 512-424-2474, Option 1

# Secure Site

## Supervisors – Disable Users and Expired Supervisors

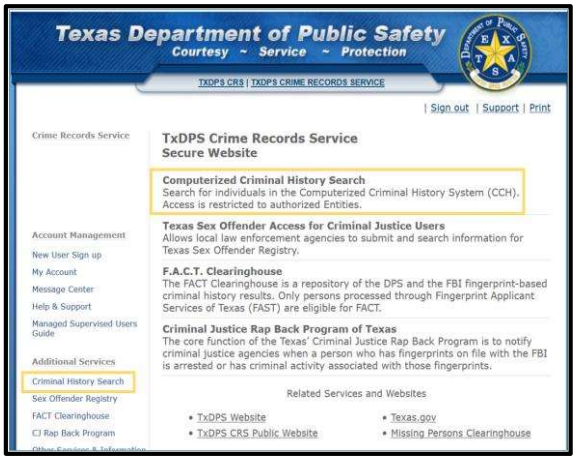
My Account

1. Organization Profile (View/Update)
2. Find user and select "Detail"
3. Select "Disable by User"
4. **Contact Criminal History Inquiry Unit at NCJU@dps.texas.gov or 512-424-2474, Option 1**

Supervisors can disable users following the information on that page to contact CHIU to finalize.
Expired Supervisors will disable all users under them – contact CHIU

# Secure Site

## Name Based Searches

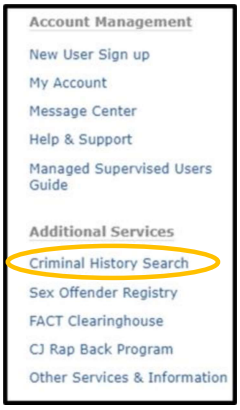



This is our CCH system, it provides Texas records only and does not create subscriptions. Searches done in this system must be logged.

# Access to CHRI

## Name-Based (Computerized Criminal History Search)

- Name-based searches are Soundex **TEXAS only** searches
- An application must be received prior to searching an individual (*Civil purpose only does not apply to CJ purposes*)
- 4.2.5.1 Justification - All users shall provide a reason for all inquiries
  - CCH Verification forms or CCH logs
  - CCH verification form is not a consent form
  - Keep form or log for audit purposes
- Name-based searches cannot be disseminated
  - Fingerprint results are true identity
  - TXI Review




TXI Reviews can be used to verify identity or if you have question about the CHRI of the applicant, can also be used if applicant wants a copy of their own CHRI. This is an alternative to the FACT clearinghouse that does not create a subscription.

# Access to CHRI

**DPS Computerized Criminal History (CCH) Verification**

(AGENCY COPY)

I, JOHN DOE, acknowledge that a Computerized Criminal
APPLICANT or EMPLOYEE NAME (Please print)
History (CCH) check may be performed by accessing the Texas Department of Public Safety Secure Website and may be based on name and DOB identifiers. (This is not a consent form, but serves as information for the applicant.) Authority for this agency to access an individual's criminal history data may be found in Texas Government Code 411; Subchapter F.

Name-based information is not an exact search and only fingerprint record searches represent true identification to criminal history record information (CHRI), therefore the organization conducting the criminal history check is not allowed to discuss with me any CHRI obtained using the name and DOB method. The agency may request that I also have a fingerprint search performed to clear any misidentification based on the result of the name and DOB search.

In order to complete the fingerprint process I must make an appointment with the Fingerprint Applicant Services of Texas (FAST) as instructed online at www.dps.texas.gov/*Crime Records Information/Review of Personal Criminal History* or by calling the DPS Program Vendor at 1-888-467-2080, submit a full and complete set of fingerprints, request a copy be sent to the agency listed below, and pay a fee of $25.00 to the fingerprinting services company.

Once this process is completed the information on my fingerprint criminal history record may be discussed with me.

**(This copy must remain on file by this agency. Required for future DPS Audits)**

Signature of Applicant or Employee (optional)

Date

123 AGENCY
Agency Name (Please print)

HUNGRY HIPPO
Agency Representative Name (Please print)

HUNGRY HIPPO
Signature of Agency Representative

06/01/23
Date

Please:
Check and Initial each Applicable Space

CCH Report Printed:

YES X NO ___ H.H initial

Purpose of CCH: Applicant: Administrator

Empl X Vol/Contractor ___ H.H initial

Date Printed 06/01/23 H.H initial

Destroyed Date 06/02/23 H.H initial

Retain in your files

**CCH Verification Log- Non Criminal Justice**

| NO. | Search Date | NAME | Purpose of CCH | Reference # | CCH Printed | | INTL: | Date Printed | Date Destroyed | INTL: |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 06/01/23 | JOHN DOE | Applicant: Administrator | 123 | □YES | ☑NO | H.H | | | |
| 2 | 06/01/23 | JANE DOE | Applicant: Administrator | 123 | ☑YES | □NO | H.H | 06/01/23 | 06/01/23 | H.H. |
| 3 | | | | | □YES | □NO | | | | |
| 4 | | | | | □YES | □NO | | | | |
| 5 | | | | | □YES | □NO | | | | |
| 6 | | | | | □YES | □NO | | | | |

**Criminal Justice CCH Verification**

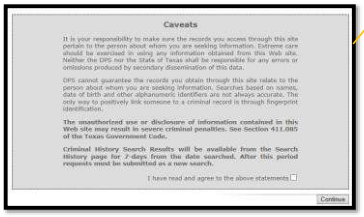
| Search Date | NAME | Purpose of CCH | Reference # | CCH Printed | | INTL: | Date Printed | Date Destroyed | INTL: | Requested By | Provided To |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 6/1/2023 | John Doe | Employment Applicant: Police Office | 1234 | | □ NO | H.H | | | | | |
| 6/1/2023 | John Doe | Employment Applicant: Police Office | 123 | □ YES | | H.H | 6/1/2023 | 6/2/2023 | H.H | | |
| 6/1/2023 | John Doe | Criminal Justice Purpose: Case#1232 | 1232 | □ YES | | H.H | 6/1/2023 | | H.H | Austin PD | Investigator Gator |
| | | | | □ YES | □ NO | | | | | | |

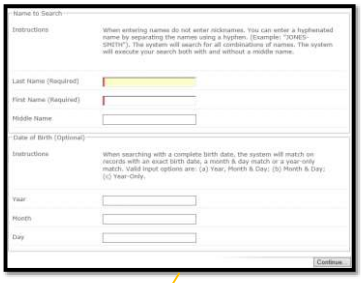
To prepare for the audit make sure you have each one of your searches logged and have some sort of documentation to proof purpose.
Ex: Job applications, payroll, job offer

# Secure Site

## Name-Based Searches

- Navigation Area
  1. Criminal History Search
  2. Search Database
  3. Read and agree Caveats
  4. Begin name-based search



Search identifier is optional but can be helpful come audit time.

# Security and Storage

## Physical Media

- Printed and stored CHRI will need to be locked at all times. Only **authorized individuals** shall have keys for locked CHRI.
  - Do not comingle CHRI in personnel files.
  - Do not keep/store any physical CHRI, we recommend disposing once your decision has been made. FACT Clearinghouse is live data, storage is not necessary/recommended.
  - **Criminal History Record Information (CHRI)** — A subset of CJI. Any **notations** or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges
    - Recommend not keeping any kind of log tracking an individual's criminal history search results .
    - Recommend not keeping any file management with notations about criminal history.
    - Recommend not keeping any "passed or failed criminal history check" lists or checklist
    - **If you keep any of the listed, you must treat them as CJI and retain/secure according to your statue and CJIS SP.**
    - Electronic retention of CHRI shall be encrypted with passphrase. (5.10.1.2.2)

We are talking about building access inside and out.
If your statute allows for the retainage of CJI then it must be secured at all times
Comingling – separate files, our CHRI from our site is not subject to open records or court orders.
Transporting – should not be needed. No offsite storage allowed.

# Security and Storage

## Digital Media – Part 1

- **If stored electronically within desktop, database, network, cloud, and email. All will need to be encrypted with FIPS 140-2 / 197. CHRI shall be encrypted during transit and at rest.**
  - IT personnel will need to be fingerprinted. (If 411 permits or TXI Review)
  - Only authorized individuals shall have access to the encryption keys.
  - CHRI will need to be in a File Management. Do not create a mass storage or database.
  - Firewall and Anti-Virus in place with current version.
  - Encrypt CJI prior to uploading to cloud.

- **Windows Vista, Windows XP, Windows 7, and Windows 8** are EOL-End of Life, they shall not be used for access and storing CHRI. (CSP 5.10.4.1)
- **macOS 10.15 (Catalina), macOS 10.14 (Mojave), macOS 10.12 (Sierra)** and older are EOL-End of Life, they shall not be used for access and storing CHRI. (CSP 5.10.4.1)

# Security and Storage

## Digital Media – Part 2

- Apply routine patches to all software or components in a timely manner. (CSP 5.10.4.1)
- CHRI Shall not be accessed from public computers.
- If the Secure Site is accessed by mobile devices from the agency, implement the following;
  - VPN – Virtual Private Network (Laptops)
  - Restrict WiFi
  - Monitor and control wireless access.
  - Application that prevents CJI to be shared on personal applications. (Facebook, Twitter, etc.)
  - Application for IT personnel to disable wireless device if lost or stolen.
  - Mobile Device Management (Smartphones and Tablets)
  - 5.5.6.1 : BYOD (bring your own device) Shall have agency established and documented terms and Conditions and controlled per CJIS 5.13 requirements

# Sanitization and Destruction

## Physical Media

- If printed, we recommend you destroy after decision has been made otherwise it has to be treated as CJI and you must follow retention/storage as outlined by your statue and CJIS Security Policy.
- Shred, pulverize, or incinerate printed CHRI **in-house**.
- Destruction shall be done or witnessed by authorized individuals, **otherwise an Outsourcing Standard Agreement should be in place.**
  - Criminal Justices agencies must have MCA or SA in place.

## Digital Media

- Sanitize or destroy all digital media containing CJI when it's inoperable or will no longer be used by the authorized agency.
  - Computers
  - Laptops
  - Tablets
  - Smartphones
  - Network Printers
- Sanitization and Destruction shall be done or witnessed by authorized individuals.
- **Recommend not to** store anything from the FACT Clearinghouse electronically.

This is all required to be in your agency's CJI Policy - in the FBI Sample Policy in the Launch Pad that you may adopt
Check your statute for retention – preferably, do not save – everything is live in FACT and the records will update, the second you print that record is stangnat and out of date.
3rd party is not to shred onsite UNLESS witnessed by authorized personnel, cameras do not qualify
If taken offsite to shred, OS needed – all contractor employees need to be FP IF YOUR STATUE ALLOWS. If it does not allow then FP through personal review – not your SC for schools – expensive

So options to sanitize old equipment are to remove hard drives when necessary and physically destroy – check copier contracts for additional fees
For individuals no longer with agency, purge information unless required for retainage by your regulatory agency

# Outsourcing: Non-Criminal Justice Agencies

- All outsourced vendors will have to be vetted through TX DPS and become CJIS Security Policy approved.
- The following will need to be in place for an Outsourcing Standard:
  - Written Request Letter.
  - Copy of the contract with the vendor. It must reference the CJIS Security Policy and Outsourcing Standard Agreement.
  - A completed Outsourcing Standard.
  - Vendors will need to be fingerprinted.
- After outsource vendors are approved, agency will have to:
  - Conduct an audit within 90 days of the Outsourcing Standard Agreement approval date.
  - Report any incidents to TX DPS.
  - Keep vendors current with CJIS Security Policy.
  - Fingerprint vendor (if statue allows if not then TXI)
  - CJIS security Awareness Training
- Depending on the services, an Outsourcing Standard can be prevented if authorized personnel from the agency performs or witness the services.

# Outsourcing: Criminal Justice Agencies

- **Security Addendum or Management Control Agreement Required (IT, Storage, Data Destruction, and Retrieval)**
  - Samples available in CJIS Launchpad
  - Non-Criminal Justice Agency (Government) Ex: City/County, will require a Management control agreement (CJIS 5.1.1.4)
  - Private vendors/contractors require Security Addendum (CJIS 5.1.1.5)
- **Vendors are required to complete CJIS security awareness training and be fingerprinted**

## Public Resources

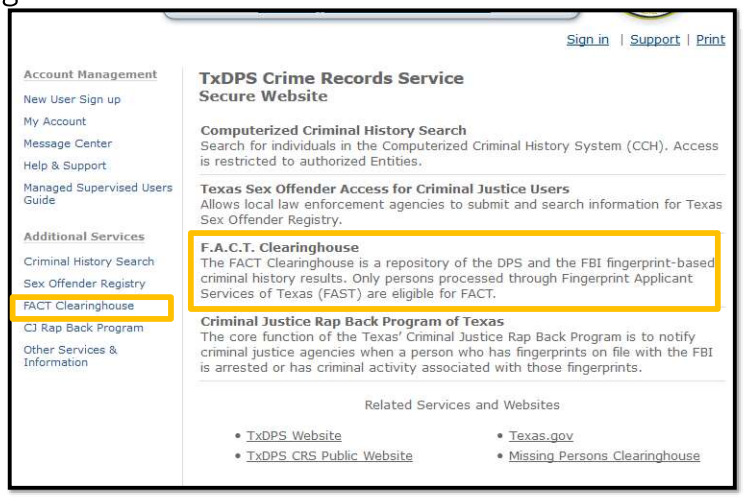
- **DPS Public Site:** Convictions or deferred adjudications that have been reported to the Department on an offense.
  - https://publicsite.dps.texas.gov/convictionnamesearch/
- **DPS Public SOR**:
  - https://publicsite.dpd.texas.gov/sexoffenderregistry/
- **TXI Review/ TXE Review**
  - dps.texas.gov/internetforms/Forms/CR-63.pdf
  - dps.texas.gov/internetforms/Forms/CR-68.pdf

If your legislative authority does not let you run a specific population, we have options to still run background checks on the public records side of DPS.

## The following is FACT Clearinghouse Only

# Secure Site

## Fact Clearinghouse



# Access to CHRI

Fingerprinting

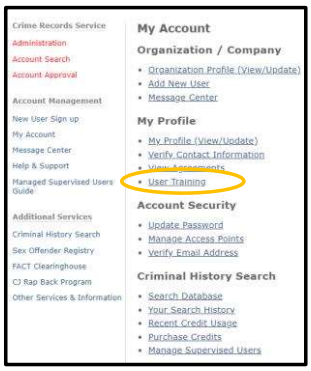
- Please ensure to use the correct Service Code and ensure your agency's Service Code is not shared
- A completed application must be received prior to fingerprinting an individual.
- You may only disseminate fingerprint results to authorized individuals & the to the individual of the record.
  - In person
  - Certified Mail
  - Secure Fax Machine
  - Do not disseminate over the phone.
  - Recommended not sending CHRI by email due to encryption requirements
  - Recommend having a release form.
- Unsubscribing to the individuals who are no longer with the agency is a requirement.
  - GC § 411.0845
  - Unsubscribe within 3 business days per the Access & Dissemination Policy.

# Required Training

CJIS Security Awareness Training is now ***ANNUAL***

| | | |
|---|---|---|
| Level 1 is now | Security and Privacy: Basic Role | **Personnel with Unescorted Access to a Physically Secure Location** (This level is designed for people who have access to a secure area but are not authorized to use CJI) |
| Level 2 &3 are now | Security and Privacy: General Role | **All Personnel with Access to CJI** (This level is designed for people who are authorized to access an information system that provides access to CJI) |
| Level 4 is now | Security and Privacy: Privileged Role | **Personnel authorized to perform security-relevant functions** (This level is designed for all information technology personnel including system administrators, security administrators, network administrator, etc...) |
| LASO | Security and Privacy: Security Role | **Organizational Personnel with Security Responsibilities** (This level is designed for personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJIS Security Policy) |

# Required Training




| Course Description | Status | |
|---|---|---|
| Criminal History - 1. Introduction and Overview | PASS | Training |
| Criminal History - 2. Account Management | PASS | Training |
| Criminal History - 3. Handling Information | PASS | Training |
| Criminal History - 4. Name-Based Searches | PASS | Training |
| Criminal History - 6. FACT Clearinghouse | PASS | Training |

## Secure Site Training Modules

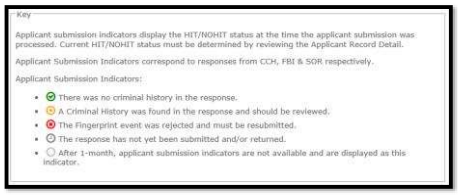
- All modules must be completed prior to usage of the Secure Site.
- Depending on the status of the user, some will take more modules than others.
- Modules will train the user how to use the Secure Site.
- It is a one-time exam per module unless there is an update. You may review modules at anytime.

# Secure Site

## Clearinghouse - Worklist

### Navigation Area

- Fact Clearinghouse
- View Worklist
  - Select a worklist to view



- Click Detail to View Record
- Click Close to remove from the "Worklist" (Close button will NOT unsubscribe)

So all users that access the FACT should know how to use their Worklist and should visit it regularly this is where you are updated live about your subscriptions.

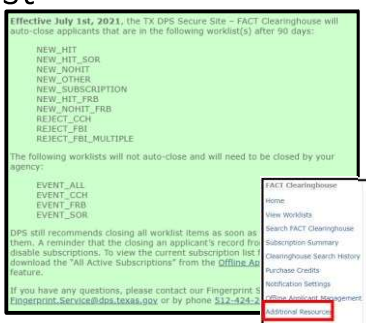
Use this Worklist as a Notification Center. When ever you receive an email letting your know there has been an event in someone's Fingerprint you would log into the FACT and review the information.
After reviewing you should close out this notification in Worklist. Closing the notification is not going to unsubscribe.

# Secure Site

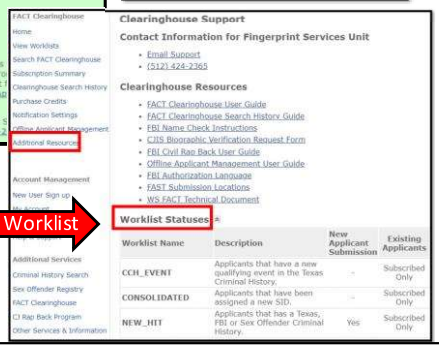
## Clearinghouse - Worklist

### Navigation Area

- Fact Clearinghouse
- Closing from the "Worklist" **will NOT unsubscribe**




Worklists will show a maximum 500 most recent items per worklist.

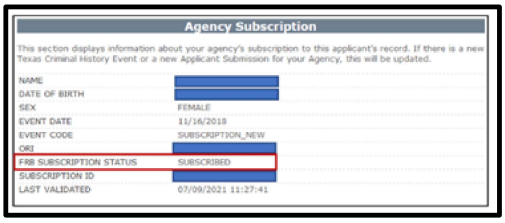



Definitions to Worklist

If you need the definitions to the worklist, we have definitions under additional resources in the FACT.

# Secure Site

## Clearinghouse – Applicant Detail Page



$1 Viewing Fee

All the information you need to verify all the information on the Detail page. Different identifiers.

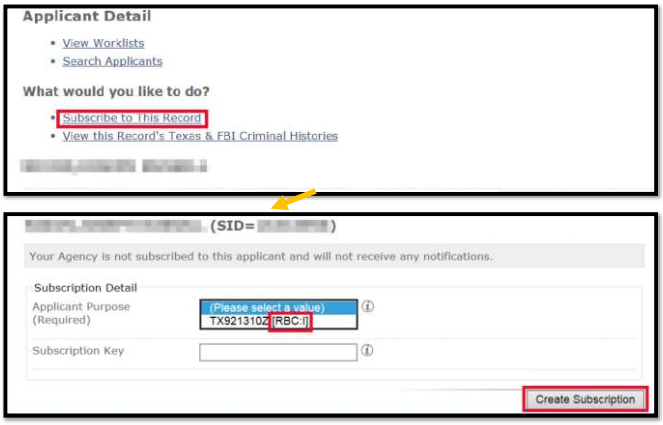
Active FBI rapback true and true, this is what you want. When you pull them in it is going to cost you $1 if you had them fingerprinted that viewing will not cost you for 30days.

# Secure Site

## Clearinghouse – **Manual** Subscriptions

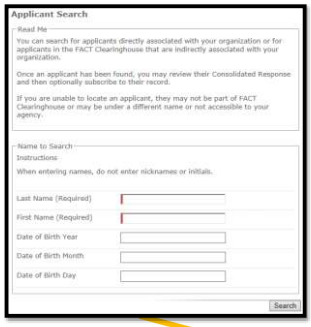
- Navigation Area

1. **FACT Clearinghouse**
2. **Search Fact Clearinghouse**
   - Search by name, SID, DL, or MNU (Identifier from agency)
3. **Select Individual**
   1. Select "Subscribe to This Record"
   2. Click tab for Applicant Purpose and select ORI with [RBC:I] or [RBC:J] to send an FBI Rap Back request.
   3. An ORI without [RBC:I] or [RBC:J] will only receive Texas live records.
   4. Select "Create Subscription"




If you are creating a manual subscription meaning the applicant has been fingerprinted before for the SAME purpose you need to make sure you see RBC if you see and ORI with no RBC after it that means you are only receiving Texas records.
Ex: Police officer coming from a different PD. Teacher coming from another ISD.

# Secure Site




## Clearinghouse - Unsubscribing

### Navigation Area

- FACT Clearinghouse
- Search Fact Clearinghouse
  - Search by name, SID, DL, or Subscription Key (Identifier from agency)
- Select Individual
  - Select "Manage this Records Subscription"
  - Select Unsubscribe

# Secure Site

## Clearinghouse - Subscription List

- FRB Subscription Status

| | |
|---|---|
| NOT ELIGIBLE | The fingerprints submission for the applicant was processed prior to June 1st, 2015 or they were rejected by the FBI. The FRB subscription cannot be created until the applicant is re-fingerprinted and accepted by the FBI. |
| ELIGIBLE | The fingerprints submission for the applicant is eligible for an FRB. The eligible fingerprints will be submitted to the FBI once the FBI initial response is received or when manually creating a subscription.<br><br>The fingerprints that were submitted and did not automatically enroll for the FBI Civil Rap Back Program between June 1st, 2015 and January 15th, 2018 are also eligible. Contact the Fingerprint Services Unit to enroll the applicants to the program. 512-424-2474 – Option 6 |
| PENDING | The eligible fingerprints submission from the applicant has been submitted to the FBI to create the FRB subscription. |
| SUBSCRIBED | Confirmation that the FRB subscription has been established for the agency and is active. |

| F | G | H |
|---|---|---|
| HasTexasSubscription | FRB Subscription Status | FP Date |

| F | G | H |
|---|---|---|
| HasTexasSubscription | FRB Subscription Status | FP Date |
| Y | NOT ELIGIBLE | 1/12/2015 4:51:32 PM |
| Y | SUBSCRIBED | 7/31/2018 7:14:23 PM |
| Y | SUBSCRIBED | 9/15/2020 6:20:32 PM |
| Y | SUBSCRIBED | 8/25/2015 2:35:05 PM |
| Y | ELIGIBLE | 9/23/2016 3:22:30 PM |
| Y | SUBSCRIBED | 7/6/2021 4:45:02 PM |
| Y | NOT ELIGIBLE | 9/16/2013 6:35:29 PM |
| Y | NOT ELIGIBLE | 12/2/2016 3:21:06 PM |
| Y | SUBSCRIBED | 3/9/2021 6:35:46 PM |
| Y | SUBSCRIBED | 8/4/2016 1:38:54 PM |
| Y | NOT ELIGIBLE | 11/10/2010 9:10:32 AM |
| Y | NOT ELIGIBLE | 4/27/2015 4:37:39 PM |
| Y | SUBSCRIBED | 8/10/2020 10:35:34 PM |
| Y | ELIGIBLE | 9/23/2016 3:07:50 PM |
| Y | NOT ELIGIBLE | 9/13/2016 7:35:45 PM |
| Y | NOT ELIGIBLE | 10/25/2010 9:01:47 PM |
| Y | SUBSCRIBED | 8/20/2020 4:52:29 PM |
| Y | SUBSCRIBED | 3/1/2019 2:24:19 PM |
| Y | SUBSCRIBED | 7/15/2019 3:24:30 PM |
| Y | SUBSCRIBED | 8/13/2018 4:16:31 PM |
| Y | SUBSCRIBED | 4/6/2020 9:48:06 AM |
| Y | NOT ELIGIBLE | 5/28/2015 5:18:59 PM |
| Y | NOT ELIGIBLE | 4/22/2016 8:49:02 AM |
| Y | NOT ELIGIBLE | 11/27/2013 12:43:51 AM |
| Y | ELIGIBLE | 9/30/2016 10:11:28 PM |
| Y | NOT ELIGIBLE | 7/16/2016 8:18:05 AM |
| Y | SUBSCRIBED | 3/5/2019 2:19:50 PM |
| Y | NOT ELIGIBLE | 9/21/2010 7:27:13 AM |
| Y | SUBSCRIBED | 11/8/2019 2:27:46 PM |

You need to address all the names on your list that have a "Pending" status by calling FSU and you will have to get "Not Eligible" status individuals re-fingerprinted.

# Secure Site

## Clearinghouse – Fingerprints Rejection Message

| SUBMISSION DATE 07/07/2018 | |
|---|---|
| ORI | TXFACTV0Z |
| NAME | [redacted] |
| BIRTH DATE | [redacted] |
| DL NUMBER | [redacted] |
| MNU | |
| DPS TCN | [redacted] |
| FBI TCN | E2018[redacted] |
| SEX | FEMALE |
| CRS/CRT | NONE/NONE |
| FRS/FRT | NONE/NONE |
| FBI TEXT | L0008 - THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED. |

Pay Attention to the FBI Text for rejected fingerprints.

| | |
|---|---|
| FRS/FRT | DONE/REJECT |
| FBI TEXT | L0008 - THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED.. CANDIDATE(S) WERE FOUND. PLEASE RESUBMIT A NEW SET OF FINGERPRINTS FOR COMPARISON TO THE CANDIDATE(S). |

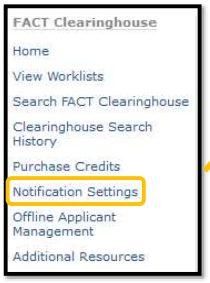
| | |
|---|---|
| FRS/FRT | NONE/NONE |
| FBI TEXT | L0117 FINGERPRINT IMAGE DOES NOT CONTAIN SUFFICIENT VISIBLE PATTERN AREA IN ROLLED AND/OR PLAIN IMPRESSION BLOCK(S). SEE FINGER(S). 1-10 CANDIDATE(S) WERE FOUND. PLEASE RESUBMIT FOR COMPARISON TO THE CANDIDATE(S). |

They go back a second time within 6 months to reprint with no fee. After that they have to start the whole process over. If there is a 2nd reject, they need to request a NB search from FBI.

# Secure Site

## Clearinghouse - Notification Settings

- Navigation Area
  - FACT Clearinghouse
    - Notification Settings

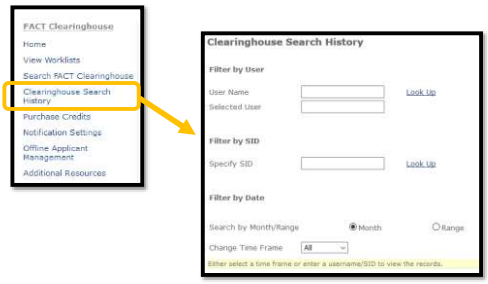


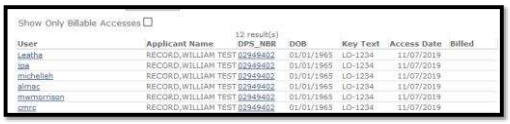
- Sub – New Subscriptions.
- Data – Events

# Secure Site

## Clearinghouse Search History

- The FACT Clearinghouse Search History allows agencies to monitor the views that are being processed by their data users on the TX DPS Secure Site. In addition to monitoring the views, it will show which views incurred a fee for your agency.




When utilizing any of the search options, a checkmark ( ✓ ) will appear in the column "Billed" for any of the searches that were charged to the agency. Select "Show Only Billable Accesses" to only view the searches that were billed.

# Audit

- TX DPS and FBI Audit – Every 3 years
- 2 Types of audits
- Onsite
  - Split into 2 parts:
    1. Electronic part
       - Electronic questionnaire, electronic records verification, supporting docs requested by auditor
    2. Onsite part.
       - Onsite Inspection
- Electronic Audit
  - All information will be submitted to auditor electronically and will require additional items, an example of this is these audits require pictures of secure areas, workspaces and floor layout.
- Who Should Attend Onsite Audit?
  - Account Supervisor for Secure Site
  - Data Users (optional)
  - IT personnel (optional)
  - If needed, you may include individuals who make the decisions for the agency. (example: Directors, Managers, and Supervisors)
- Time Frame for Audit
  - An onsite audit will average 2 hours long.
    - It can last longer if the agency has additional questions or requires additional training.
  - The electronic process will be assigned a 7-business day deadline to respond to the audit findings.

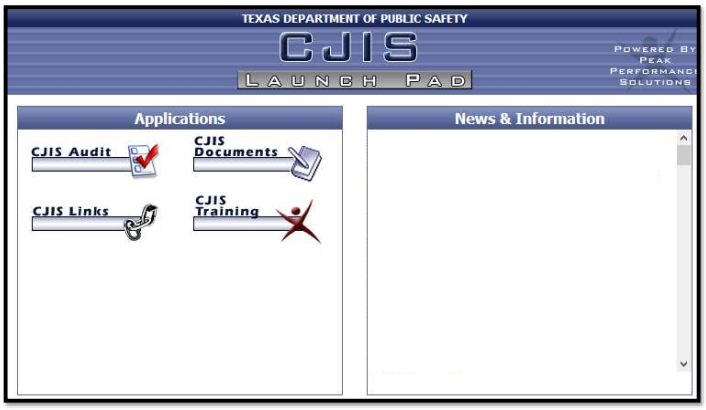
# Audit

## Compliance Tips

- Become familiar with the Launch Pad.
- Have agency policies regarding the use of CHRI per the Access & Dissemination Policy and the CJIS Security Policy.
- Take the required trainings.
- Keep justification of why CCH was searched for a minimum of audit to audit (3 years).
- Have a procedure for unsubscribing within 3-business days.
- Ensure the security of physical and electronic CHRI.

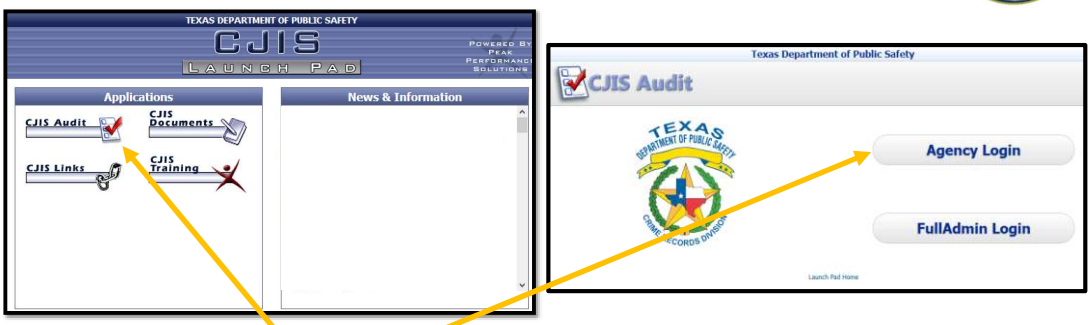
# CJIS Launch Pad

https://texas.cjisapps.com/**noncrim**/launchpad/




CJ agencies you might have other launchpads this one is specifically for the civil side please make sure you bookmark us as "nonCJ". This launchpad is public and does not have a log in, do not try to google it, it will take you to a different launchpad.

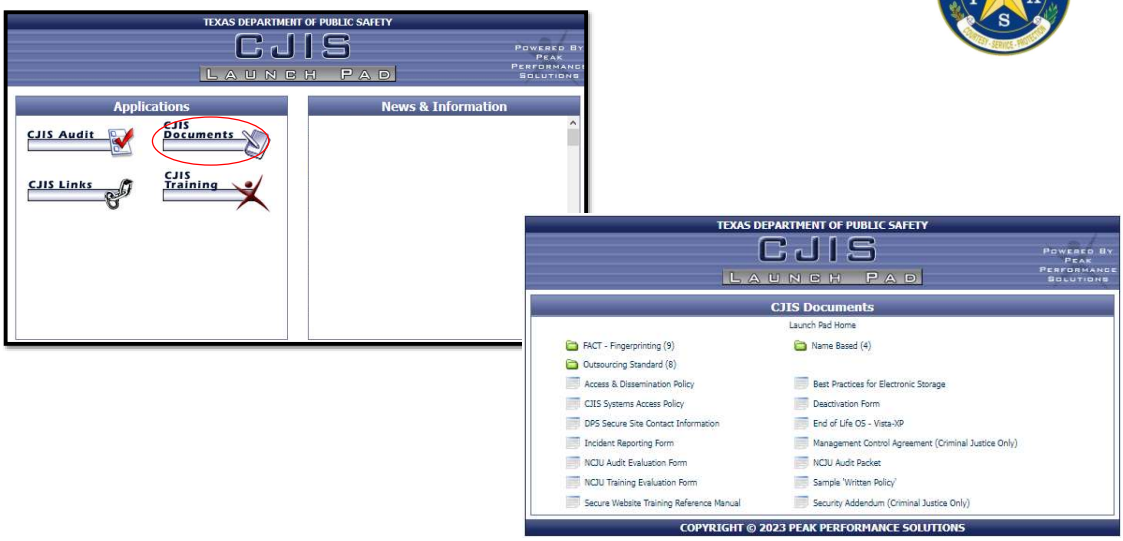
# CJIS Launch Pad - Audit




- Electronic portion of the questionnaire.
  - You are able to log in as many times as you need to complete or view your current or past questionnaires.

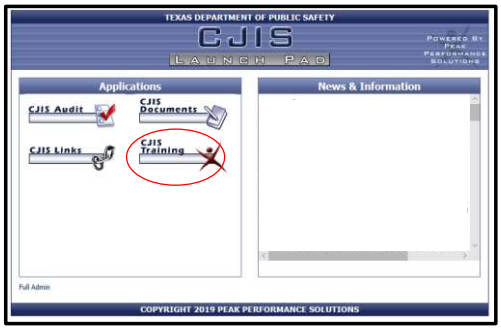
Give us a call if you cannot log in and we can reset your login.

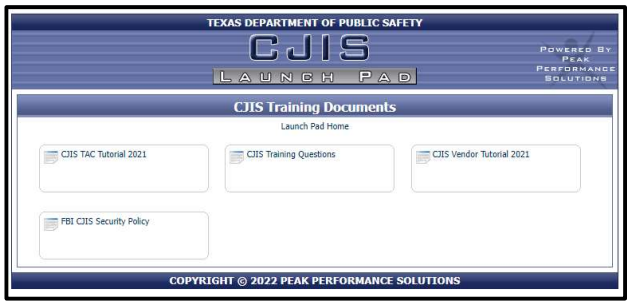
# CJIS Launch Pad - Documents




Recommend printing/saving:
NCJU Audit Packet
Sample Written Policy
Incident Reporting Form
Contact Information

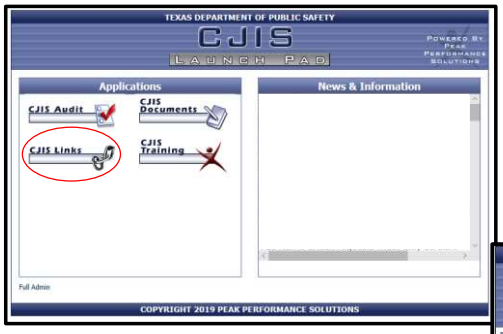
# CJIS Launch Pad - Training




Has TAC Tutorial
After first test completed – system will take over notifications
TAC ADMIN GUIDE is wrong!

# CJIS Launch Pad - Links



CJIS online

# Crime Records Link

http://www.dps.texas.gov

Has CRD information for us and other CRD units.

# Contacts

**Criminal History Inquiry Unit**
Email: NCJU@dps.texas.gov
Phone: 512-424-2474, option 1 & 2

**Audit and Training Unit**
Email: CJIS.Audit@dps.texas.gov
Phone: 512-424-2474, option 3

**Billing Unit**
Email: CRS.Billing@dps.texas.gov
Phone: 512-424-2474, option 4

**ADB Support Unit**
Email: ADBSUPPORT@dps.texas.gov
Phone: 512-424-2474, option 5

**Fingerprint Services Unit**
Email: Fingerprint.Service@dps.texas.gov
Phone: 512-424-2474, option 6

These all the units that would together to make sure we can assist you.

- Fingerprint Services Unit: Helps with fingerprint rejects, problems with the FACT clearinghouse, service codes and FRB status problems.
- Criminal History Inquiry Unit: Open/Closes accounts, adds/removes users, unlocks accounts, helps with legislative authority.
- Billing Unit: Billing issues if your agency gets billed.
- ADB Support Unit: Fingerprinting vendors, locations, complaints, suggestions.

# Leave us a review!