State of Connecticut
FBI CJIS Security Policy
2021 Security Awareness Training
For
Noncriminal Justice Agencies

This Security Awareness Training is based on the

United States Department of Justice

Federal Bureau of Investigation (FBI)

Criminal Justice Information Services (CJIS) Division

CJIS Security Policy

Version 5.8

CJISD-ITS-DOC-08140-5.8

June 1, 2019

FBI CJIS Security Policy

The FBI CJIS Security Policy is the minimum security standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division.

The CJIS Security Policy:

- Applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information;
- Provides the appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit;
- Provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI; and
- Can be found on the FBI.gov website and may be posted and shared without restrictions.

Security Awareness Training

The FBI CJIS Security Policy requires all personnel, with access to criminal justice information (CJI) in any form, to complete Security Awareness Training within six (6) months of initial assignment and biennially thereafter.

This training is designed to provide security awareness training to agencies with access (physical and logical) to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes. As required by the FBI CJIS Security Policy, this includes:

- Personnel who are authorized to obtain, review, copy, file, or otherwise handle CJI;
- Higher level agency heads who may view CJI;
- Vendors and anyone who works on/maintains a technical component that is used to send, receive, process or route a transaction to/from systems that processes or maintains CJI; and
- Personnel with unescorted access to physical security locations that may store or contain CJI.

Noncriminal Justice Purposes
The use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Physical Access
The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Logical Access:
The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Introduction to the National Identity Services Audit

In October 2014, the FBI started cycle 0 audits on agencies with access to CHRI for noncriminal justice purposes. Audits assess compliance with the COLLECT System (if applicable), International Justice and Public Safety Network (NLETS), FBI CJIS, and National Crime Prevention and Privacy Compact Council (Compact Council) policy and regulations.

Federally Mandated Formal Audits:

- All user agencies must be audited at least once every (3) three years by the Department of Emergency Services and Public Protection, Division of State Police. There are two audit programs. The audits assess compliance with National Identity Services (NIS) standards and CJIS Security Policy Information Technology Security (ITS) standards.

- A randomly selected group of user agencies will be audited at least once every (3) three years by the FBI CJIS Audit Unit. Selected agencies will be subjected to a NIS and ITS Audit.

- More frequent audits may occur as a result of possible system violations.

- Unannounced security inspections and scheduled audits of contractor facilities may be conducted.

Definition of Criminal History Record Information

CJI is sensitive and confidential data and should be treated as such.

- Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

- Any FBI data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history that may include personally identifiable information (PII).

- 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.

- Any information that confirms the existence or nonexistence of a criminal record.

- Information is considered CHRI if it is transferred or reproduced directly from CHRI and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format.

- This includes **applicant status information**, which is either directly attributed to or predominately based on a national FBI check, when no authority or inherent need exists for the release of such information.

- *Examples of formal and informal products or verbalizations include: correspondence such as letters and e-mails; documents such as forms and hand-written notes (including notes on posted notes); conversations either in person or by telephone; and data fields such as those stored in database tables or spreadsheets*.

Authorized Access

The FBI provides a means of conducting national criminal history record searches for noncriminal justice purposes as authorized by federal statutes, Executive Orders, and state statutes approved by the Attorney General of the United States.

A purpose or need for use is a request for CHRI to adjudicate a specific application for a noncriminal justice purpose (e.g., license, position of employment, benefit, etc.) that is known at the time the request is made, pursuant to an approved statutory authority, and based on the positive identification via fingerprint submission of the applicant.

Each statutory authority defines the specific purposes (applicant types) for which CHRI may be requested and used.

When CHRI is needed for a subsequent **authorized use**, a new record request must be conducted to obtain current information, if authorized by state or federal law.

To ensure that a specific category of applicants is authorized for a national background check, the statutory authority must be closely reviewed.

Basic Parameters for Use

The basic parameters for use consists of (chronologically):

Approved Statutory Authority	• There must be an approved state statute, federal statute, or Executive Order and approved by the Attorney General (AG) of the United States. • The AG's approval authority is delegated to the FBI by Title 28, CFR, §§ 0.85(j) and 50.12(a).
Authorized Recipient	The agency must be designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions.
Authorized Use/Purpose	• The agency must be able to prove that the applicant met the statutory requirement to be fingerprinted, under the approved state statute, federal statute, or Executive Order. • This supporting documentation (application or letter of hire) must be retained for at least one (1) year, regardless if the applicant was not hired or denied.
Fingerprint submission	• All applicants must receive the Noncriminal Justice Applicant Privacy Rights Form and FBI Privacy Act Statement, prior to being fingerprinted. • The Reason Fingerprinted Field (RFP) or "Applying For" section of the fingerprint card must contain the correct statutory authority and specific position that the applicant is applying for. • The National Child Protection Act/Volunteer for Children's Act (NCPA/VCA) Notice and Consent Form is required for persons fingerprinted under the NCPA/VCA.
Receipt of CHRI	Electronic and hardcopy forms of CHRI must be protected pursuant to the FBI CJIS Security Policy Compact Council rules and regulations.
Adjudication or fitness determination	• The agency must meet Privacy Requirements for Noncriminal Justice Applicants. • This is a federal requirement and failure to do so may result in a civil actions.
Closing or maintenance activities	Information must be properly secured until retention is no longer required by state or federal law and then properly destroyed pursuant to the FBI CJIS Security Policy.

Physical Protection

Physical Protection Policy must ensure CJI and information system hardware, software, and media are physically protected through access control measures. At a minimum, the agency must designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage.

Minimum Security Requirements

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI;

2. Lock the area, room, or storage container when unattended;

3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view; and

4. Follow the encryption requirements for electronic storage (i.e. data "at rest") of CJI in the FBI CJIS Security Policy.

Additionally:

- Security perimeters must be defined, controlled and secured.
- A current a list of personnel with authorized access to the CJI must be developed, maintained, and available upon request for auditing purposes.
- Individual access authorizations must be verified before access is granted.
- Physical access to the information systems (such as desktop computers, communications closets/rooms, unencrypted communication lines, physical records, etc.) must be monitored to detect and respond to physical security incidents.

Physical Protection & Individual Accountability

- **Not only is it required per CJIS Policy, it is each individual's responsibility to protect CJI with all due diligence. Even the most technically and physically secure environments are subject to threats due to lack of due diligence and/or inappropriate conduct from the insider.**
- All authorized individuals are subject to the agency physical protection policy to ensure that the security of CJI is maintained.
- All individuals need to remain cognizant of the designated physically secure areas and ensure that all personnel abide by access control points, entrance and exit procedures, visitor control and handling procedures.
- All individuals need to maintain vigilance in recognizing individuals who may not have appropriate access and may have been left unescorted.
- Visitors must be authenticated before escorted access to a secure location can be authorized. Visitors must be escorted at all times. An escort is an authorized individual who accompanies a visitor at all times while within a secure location to ensure the protection and integrity of the secure location and any CJI therein. The use of cameras or other electronic means used to monitor a secure location does not constitute an escort.
- All individuals should report areas of sensitive access that may be unsecure such as emergency exit doors which may have been left propped open.
- All authorized individuals must ensure that CJI, whether in physical or electronic form, remain in the secured areas unless they have specific authorization and procedures for taking that information out of the secure area.
- **Physical security incidents or possible security incidents must be reported to the Terminal Agency Coordinator (TAC) in a timely manner. The TAC is the designated point-of-contact for matters relating to CJI at the local agency. These incidents can also be reported to the Connecticut CJIS Systems Officer (CSO).**

Media Protection

Media Protection Policies must ensure that access to media (physical and digital) in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Digital media refers to any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Minimum Security Requirements

Storage and Access: Agencies must securely store physical or digital media within physically secure locations or controlled areas. The agency shall restrict access to authorized individuals.

Transport: Agencies must protect and control physical or digital media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Physical Media Disposal: Physical media must be securely disposed of when no longer required, using formal procedures. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Digital Media Destruction: Agencies must sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. All sanitization and destruction procedures must be witnessed or carried out by authorized personnel.

Media Protection & Individual Accountability

- CJI can be leaked inadvertently outside the confines of secured areas when proper handling and marking procedures are not followed.
- All physical forms of CJI should be clearly marked and labeled ensuring documents are maintained according to policy and procedures. It is highly recommended that documents, at a minimum be clearly labeled.
- Coversheets designating the sensitive nature of the data and user responsibility in handling that data should also be considered as an appropriate measure.
- Electronic forms of media can become mishandled rather quickly due to the hidden nature of the data. Optical media and flash drives should be clearly labeled especially given those forms of media that are not protected by encryption.
- When email contains sensitive information, it should be standard practice to label those items as well and to ensure transmission is encrypted when applicable.
- Encryption is the only approved method for email traffic containing CJI.
- Users must protect their passwords accordingly, not sharing their individual account access or allowing for the possibility of compromise. All passwords must follow secure password attributes as listed in the CJIS Security Policy.

Malware & Social Engineering

Malware

All users should remain cognizant that their workstations and portable devices are actively being protected with Antivirus/Malicious Code Protection software (per the implementation of the IT staff and local policy and procedures). While this can be mainly automated (via auto update features) for internal systems, end-users play a crucial part in validating that antivirus definitions remain current on their systems.

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information.

Social Engineering can be accomplished via:

Pretexting: the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances… or

Phishing: e-mail that appears to come from a legitimate business—a bank, or credit card company— requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN. Phishing can also be facilitate over the phone and Interactive Voice Response.

Common Technical Threats

Groups, individuals, devices, systems, and services are increasingly being targeted by both foreign and domestic malefactors. Hardware and applications may become compromised therefore personnel operating criminal justice information systems and services require vigilance and need to quickly identify, respond and report incidents as will be discussed later in this training.

Personnel should be familiar with the following common technical threats to system confidentiality:

Viruses. A virus self-replicates by inserting copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program. Viruses can be divided into the following two subcategories:

Worms. A worm is a self-replicating, self-contained program that usually executes itself without user intervention.

Trojan Horses. A Trojan horse is a self-contained, non-replicating program that, while appearing to be benign, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to hosts. They often deliver other attacker tools to hosts.

Blended Attacks. A blended attack uses multiple infection or transmission methods. For example, a blended attack could combine the propagation methods of viruses and worms.

Security Incident Indicators

Users may only see indicators of a security incident. The following is a partial list of incident indicators that deserve special attention from users and/or system administrators:

- The system unexpectedly crashes without clear reasons
- New user accounts are mysteriously created which bypass standard procedures
- Sudden high activity on an account that has had little or no activity for months
- New files with novel or strange names appear
- Accounting discrepancies
- Changes in file lengths or modification dates
- Attempts to write to system files
- Data modification or deletion
- Denial of service
- Unexplained poor system performance
- Anomalies
- Suspicious probes
- Suspicious browsing

Dissemination

The exchange of CHRI is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

CHRI may only be disseminated to entities that are authorized to receive it relative to the state or federal statutory authority used to submit the fingerprint check.

The concept of dissemination applies to making CHRI available to recipients through physical or electronic access. The overarching requirements associated with dissemination of CHRI apply regardless of whether CHRI is "pushed" to recipients or "pulled" by recipients since the end result is the same.

CHRI must be maintained in such a manner as to not result in unauthorized access. Unauthorized dissemination can occur when "recipients" are given access to CHRI, regardless of whether or not the access was intentional.

Access to CHRI must be limited to the minimum necessary sub-offices and personnel within a department or agency that are actually required for a particular use. While authorized receiving agencies may exercise some level of discretion and freedom of maneuver to distribute CHRI within their organizational structure, they must be able to demonstrate a reasonable need for doing so.

For example, a local board of education may be designated as an authorized recipient of CHRI for the purpose of conducting background checks for prospective teachers. CHRI is stored as part of an electronic personnel records management system, accessible by all board of education employees. Although the board of education is an authorized recipient, access to CHRI must be limited to personnel within the human resources department responsible for making fitness determinations.

This will also limit the boards of educations exposure to the inherent risks associated with unauthorized dissemination of CHRI and violation of the prospective teacher's privacy rights.

Dissemination & The Subject of the Record

Agencies may disseminate ***fingerprint-based*** criminal history obtained for noncriminal justice purposes to the subject of the record only. This is permissible only for review and possible challenge to a decision made based on CHRI obtained.

Agencies cannot initiate national criminal history record checks for the sole intended purpose of providing a subject a copy of his/her record for review or challenge.

CHRI cannot be disseminated to spouses, other household or family members, or other parties such as potential employers, even at the subject's request.

CHRI ***can*** be disseminated to an attorney acting on subject's behalf when the applicant is challenging the agency's decision based on the CHRI obtained. The identity of the attorney and applicant must be satisfactorily established.

If an inherent need exist to advise a particular entity not otherwise authorized relevant to the federal statutory authority being leveraged for the national criminal history check, then it is acceptable to notify the entity of the outcome of applicant fitness determinations. Entities to which an applicant is seeking employment or licensing may receive status notifications which indicate the positive or negative outcome of fitness determinations.

Status notifications:

- Cannot confirm the existence or non-existence of a federal record;
- Must contain generic "pass/fail" language to the greatest extent possible, with the understanding that a reasonable balance must exist between the need to notify a potential employer and not indirectly confirming the existence or non-existence of CHRI;
- Notification language cannot directly reference that a national FBI check was conducted;
- Cannot be posted to a public website or national directory.

Dissemination & Other Agencies

CHRI cannot be re-used for subsequent unrelated needs by the original requestor/recipient.

CHRI cannot be disseminated to another recipient for subsequent unrelated re-use.

CHRI cannot be disseminated to another recipient for future anticipated uses, regardless of whether or not the needs are formally related.

CHRI cannot be disseminated outside of a state's jurisdiction.

Auditors:

Other authorized entities also include agencies which require residual access based on oversight authority and responsibility, such as the review of case files by an inspector general's office or regulatory auditors from outside the receiving organization. Such access should be limited to only the minimum level necessary to accomplish oversight responsibilities, and controls should be established to reasonably prevent unauthorized disclosure of CHRI.

Agencies must be able to provide the authority for authorized dissemination to auditors. This does not include DESPP or FBI CJIS auditors.

Dissemination & The General Public

CHRI cannot be disseminated to the general public.

This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of an adjudication process during a hearing that is open to the public.

The agency must demonstrate the following:

1) The hearing is based on a formally established requirement;
2) The applicant is aware prior to the hearing that CHRI may be disclosed;
3) The applicant is not prohibited from being present at the hearing; and
4) CHRI is not disclosed during the hearing if the applicant withdraws from the application process.

For example, a board or commission may be authorized to access CHRI, and as part of regularly scheduled meetings, applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. Agencies must be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

System Misuse

All noncriminal justice agencies have authorized access to CJI for noncriminal justice purposes pursuant to a federal law or state statute approved by the United States Attorney General. Any access and/or dissemination of CJI for other purposes are considered misuses of the system.

- Most misuse cases stem from affairs of the heart, political motivation, monetary gain, idle curiosity, or trying to "help out a friend".

- Misuse does not depend upon whether or not additional compensation was received for such unauthorized activity.

Methods of Misuse:

- Unauthorized requests, receipt, release, interception, dissemination or discussion of CJI;

- Improper use of information obtained from any CJI System and/or related applications and devices; and/or

- Violating the confidentiality of any data or record information and using it for personal purposes.

Misuse or possible misuse of CJI can be reported to the TAC or CSO.

Implications of Noncompliance

Unauthorized requests, receipt, release, interception, dissemination or discussion of CJI is considered system misuse.

Physical security violations and/or misuse of CJI can and has resulted in:

- Administrative (internal) investigations and/or sanctions;
- Termination of access to CJI for the individual user;
- Termination of access to CJI for the associated agency;
- Termination of employment or contract;
- Criminal investigations and/or arrests; and
- Prosecution and conviction for violation of state and/or federal crimes designed to protect the confidentiality and integrity of CJI.

Connecticut Computer-Related Crimes

All persons with access to CJI should be aware of Computer Related Offenses under Connecticut General Statutes (CGS) § 53a-250 through § 53a-261.

A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization.

A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services.

A person is guilty of the computer crime of interruption of computer services when he, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.

A person is guilty of the computer crime of misuse of computer system information when: (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system; or (2) he intentionally or recklessly and without authorization (A) alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system, or (B) intercepts or adds data to data residing within a computer system; or (3) he knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this subsection; or (4) he uses or discloses any data he knows or believes was obtained in violation of subdivision (1) or (2) of this subsection.

A person is guilty of the computer crime of destruction of computer equipment when he, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur.

The making of a false statement with intent to mislead a public servant in the performance of his/her official functions in violation of CGS § 53a-157b is a crime punishable by law.

Reporting Security Incidents and/or System Misuse

Security incidents and system misuse threaten the confidentiality, integrity or availability of state/FBI CJIS data. All employees, contractors and third party users are required to promptly report any security incident and/or system misuse to the TAC. All information must be communicated in a timely manner allowing timely corrective action to be taken.

Security incidents and/or system misuse may also be reported to the CSO, Darryl Hayes. Events can be reported by mail, phone, fax, and email using the information provided below:

Mailing Address

Department of Emergency Services and Public Protection
Division of State Police
Criminal Justice Business Applications Unit
1111 Country Club Road
Middletown, CT 06457

Phone
860-685-8020

Fax
860-685-8636

Email Address

Dps.collect.unit@ct.gov

Subject Title <**CJI Violation for** {insert agency name}>

Certificate of Completion

State of Connecticut
FBI CJIS Security Policy
2021 Security Awareness Training
for
Noncriminal Justice Agencies

I am aware that unauthorized requests, receipt, release, interception, dissemination, discussion or use of criminal justice information, in any form, is considered a misuse of the system and could result in: administrative and/or criminal investigations and sanctions; termination of access to criminal justice information for myself and/or the associate agency; termination of employment or contract; arrest; and prosecution and conviction for violation of state and/or federal crimes designed to protect the confidentiality and integrity of CJI.

I hereby agree not to violate the confidentiality of any data or record information that may come to my attention and will not use such information for personal purposes. **I further understand** that misuse does not depend upon whether or not I receive additional compensation.

I hereby certify that I have successfully completed Security Awareness Training as required by the FBI CJIS Security Policy.

Date:	**Email:**
Agency:	
Position/Title:	**Contact No:**
Printed Name:	
Signature:	

Email to: CT State Police: DESPP.Audits@ct.gov
Subject Line: FBI SAT for [your agency name]