CJIS Security and Privacy Training – Basic User

Welcome to the CJIS Security and Privacy Training! This training is designed for all individuals with unescorted access to a physically secure location.

This training will cover the following topics:

- Introduction
- What is CJI?
- Proper Access, Use, & Dissemination of CJI
- Physical Security
- Incident Response
- Conclusion
- Optional Confirmation Addendum

Introduction

Security and Privacy Training

All personnel whose duties require them to have unescorted access to a physically secure location that processes or stores Criminal Justice Information (CJI) must complete security and privacy training.

The FBI CJIS Security Policy requires that all personnel fitting the above criteria must complete this training:

- ***Before*** authorizing access to the system, information, or performing assigned duties
- ***Every year*** after the initial training

What is CJI?

In the United States, the individual right to privacy is protected by the US Constitution. The Privacy Act of 1974 further protects personal privacy from misuse by regulating the **collection**, **maintenance**, **use**, and **dissemination** of information by criminal justice agencies.

Criminal Justice Information

Criminal Justice Information (**CJI**) is the term used to refer to all of the FBI Criminal Justice Information Services (CJIS) Division provided data necessary for law enforcement and civil agencies to perform their work.

CJI can include any of the following types of data:

- **Biometric** (e.g., DNA, fingerprints)
- **Identity History** (i.e., “rap sheet”)
- **Biographic** (e.g., evidence tying someone to a specific crime)
- **Property** (e.g., a gun used in a crime)
- **Case History** (e.g., stolen cars, missing persons)

The National Crime Information Center (NCIC) is a computerized database of CJI available to law enforcement agencies nationwide.

Other Types of CJI

- **Criminal History Record Information (CHRI) –** CHRI is arrest-based data and any derivative information from that record (e.g., descriptive data, sentencing data, conviction status, etc.).

- **NCIC Restricted Files –** The majority of the data obtained from NCIC are restricted files. They are protected as CHRI and includes Gang Files, Threat Screening Center Files, Supervised Release Files, National Sex Offender Registry Files, Historical Protection Order Files, Identity Theft Files, Protective Interest Files, Violent Person Files, NICS Denied Transactions Files, and Person With Information (PWI) data in the Missing Person Files.
- **NCIC Non-Restricted Files –** All NCIC files which cannot be classified as CHRI or as an NCIC Restricted File are non-restricted.

Proper Access, Use, & Dissemination of CJI

Note: This section applies to the access, use, and dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties.

System Use Notification

A system use notification is a message displayed on information systems prior to accessing CJI, informing potential users of various usages and monitoring rules. If your duties require you to use systems which are adjacent to Criminal Justice Information systems, you may encounter this message. If you see this message, do not continue past this point as your CJIS Security authorization does not include accessing or viewing CJI.

Access, Use, & Dissemination Penalties

Unauthorized **requests**, **receipt**, **release**, **interception**, **dissemination**, or **discussion** of CJI is a serious violation and may result in the following:

- Criminal prosecution
- Termination of employment

Personnel Sanctions

Agencies must have a formal sanctions process for personnel failing to comply with established information security policies and procedures.

The agency will perform a formal disciplinary process for any personnel who fail to comply with the security policies and procedures. Continued misuse of CJI could result in an agency being denied access until the violations have been corrected.

Physical Security

The areas that process or store Criminal Justice Information (CJI) should be physically secure to prevent unauthorized access.

Physical Access Authorizations

To ensure physical security and prevent unauthorized access to physically secure areas, agencies must:

- Develop and maintain a list of individuals with authorized access to the physically secure location
- Issue authorization credentials (e.g., ID badges, identification cards, etc.) for access to the physically secure location

Physical Access Control

All access points to a physically secure location must be controlled, and individual access authorizations should be verified before granting access.

Physical Controls

Physical controls include:

- **Physical Access Devices –** Security devices (e.g., keyed locks, digital locks, biometric readers, card readers, etc.) should be used to prevent unauthorized users from accessing the secure area. Locks or entry codes should be changed in the event that keys are lost, entry codes are compromised, or users possessing keys or combinations are transferred or terminated.
- **Monitoring Physical Access –** Agencies should monitor physical access to physically secure locations to detect and respond to security incidents. Examples of physical access monitoring include the employment of guards, video surveillance cameras, and sensor devices.
- **Visitor Control –**Visitors should be escorted at all times, and any activity within the physically secure location should be monitored. Records of visitor access should be kept for ***one year*** and should include the visitor's name and organization of the visitor, signature, forms of identification, date of access, entry and departure times, purpose of visit, and the name and organization of individual being visited.

It is the responsibility of *all personnel* to help ensure that these areas stay secure. Be aware of the physical security precautions in place and follow these safety measures at all times.

Incident Response

Security Incidents

A **security incident** is a violation of the CJIS Security Policy that threatens the confidentiality, integrity, or availability of CJI.

Incident Response Training

Incident Response Training must be provided as part of the required security and privacy training. Users should be trained in identifying and reporting suspicious activities from external and internal sources. Subsequent training must be provided ***annually*** and ***when required by system changes***.

Reporting Security Events

Report any incidents or unusual activity to your agency contact, Local Agency Security Officer (LASO), or Information Security Officer (ISO) ***immediately***. Be sure to note the date, location, and description of the incident.

All personnel are required to report any suspected incident, regardless of how minor it might seem.

Conclusion

Thank you for reviewing the CJIS Security and Privacy Training! As a reminder, this training must be completed ***every year*** to remain compliant with the FBI CJIS Security Policy.

Questions

If you have any questions regarding the CJIS Security Policy or the expected behavior around Criminal Justice Information (CJI), talk to your Agency Contact or Local Agency Security Officer (LASO) for further information.

Next Steps

Depending on your organization's requirements, there may be additional training and/or a test to complete your certification.

Optional Confirmation Addendum

If directed to do so by your administrator, print this page and initial next to each item below to acknowledge that you agree to each statement. Then legibly print your full name and sign your name with today's date at the bottom of this page.

Note: <u>Only</u> print and sign this document if directed to do so by your administrator.

_____ I confirm that I read and understand the training above.

_____ I understand that I am not authorized to access, read, handle, or discuss Criminal Justice Information.

_____ I understand that unauthorized access, handling, or discussion of Criminal Justice Information could result in criminal prosecution and/or termination of employment.

_____

Print Name

_____ _____

Signature Date