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

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:

- **Fingerprints**
- **Personal data**
- **Property data**
- **Other information related to incidents and cases** (e.g., stolen cars, stolen guns, missing persons, etc.)

The National Crime Information Center (NCIC), located in West Virginia, is a computerized database of CJI available to law enforcement agencies nationwide. NCIC is supervised by the FBI CJIS Division, however the management of the information processed, stored, or transmitted to NCIC is a collaboration between the FBI and federal, state, local, and tribal criminal justice agencies.

Initials

_____

Proper Access, Use, & Dissemination of CJI

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 serious 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, agencies are responsible for:

- Developing and maintaining a current list and issuing credentials to personnel with authorized access to the physically secure location
- Prominently posting the perimeter of the area requiring physical security and separating it from nonsecure locations by physical controls

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

The physical controls required in order to be considered a physically secure location are:

Monitoring Physical Access

Agencies should monitor physical access to the information system to detect and respond to physical security incidents.

Visitor Control

Agencies should control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity within the physically secure location.

It is the responsibility of ***all personnel*** to help ensure that these areas stay secure. You are encouraged to be mindful of the physical security at all times.

CJIS Online — APPROVED

Initials

_____

Incident Response

Security Incidents

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

Security Incident Policy

Each agency accessing CJI must establish a written policy describing the overall incident handling procedures, how the agency performs incident reporting, and incident management procedures in the event of a security incident.

Authorized users who have direct access to CJI and all appropriate IT personnel should be aware of the agency's policy regarding possible security incidents and the proper reporting procedures within the agency.

Incident Response Training

Agencies must ensure that general incident response roles and responsibilities are included as part of required security and privacy training.

Reporting Security Events

Report any incidents or unusual activity to your agency contact, Local Agency Security Officer (LASO), or Information Security Officer (ISO) ***immediately***.

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

Security Incident Report

It is important that you include the following information in your report of the incident:

- Date of Incident
- Location of Incident
- Systems Affected
- Method of Detection
- Description of Incident
- Actions Taken/Resolution
- Date & Contact Info for Agency

Conclusion

Thank you for reviewing the 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.

PRINT NAME	SIGNATURE	DATE