FDLE Security and Privacy Training for Members with Unescorted Access to a Physically Secure Location

The FBI CJIS Security Policy requires individuals with unescorted access to a physically secure location complete Security and Privacy training before FDLE can authorize unescorted access to a FDLE facility. Additional Security and Privacy training will be required based on your job duties and access to Criminal Justice Information (CJI). Security and Privacy training is an annual training requirement.

This training will cover the following topics:

- Physical Access Authorizations
- Physical Access Control
- Monitoring Physical Access
- Visitor Control
- Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
- System Use Notification
- Personnel Sanctions
- Reporting Security Events
- Incident Response Training

What is CJI?

Criminal Justice Information, or CJI, is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions.

CJI includes the following:

- **Biometric data –** includes fingerprints, palm prints, iris scans, and facial recognition data
- **Identity History Data** - Includes criminal history data
- **Biographic Data –** Includes information about an individual related to a case not connected to identity data
- **Property data –** Includes information about vehicles and property associated with a crime when accompanied by any personally identifiable information (PII)
- **Case/Incident History** – Includes information about the history of criminal incidents

Physical Access Authorizations

FDLE buildings are considered physically secure locations. The CJIS Security Policy requires areas that process or store Criminal Justice Information (CJI) be physically secure to prevent unauthorized access.

To ensure physical security of FDLE buildings, FDLE will maintain a list of members with authorized access to FDLE buildings. The perimeter of FDLE buildings are marked indicating restricted access. Restricted areas are separated from nonsecure locations by physical controls.

Physical Access Controls
FDLE will control all physical access points and will verify individual access authorizations before granting access.

Monitoring Physical Access
FDLE will monitor physical access to FDLE information systems to detect and respond to physical security incidents.

Visitor Control
FDLE will control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). Authorized FDLE members will escort visitors at all times and monitor visitor activity within the physically secure location.

Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties

Criminal History Record Information, or CHRI, is a subset of CJI. CHRI shall be accessed and used only for an authorized purpose. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

The National Crime Information Center (NCIC), hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. The management of the information processed, stored, or transmitted to NCIC is shared between the FBI and federal, state, local and tribal criminal justice agencies.

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

System Use Notification

A system use notification is a message displayed on computer systems prior to accessing CJI, which informs users of various usages and monitoring rules. FDLE's system use notification indicates FDLE resources are for official business. Misuse of FDLE resources will result in loss of resources, disciplinary action, or criminal prosecution. Use of FDLE resources indicates member consent to restrictions/monitoring without prior notice.

Access, Use, & Dissemination Penalties/Personnel Sanctions

Unauthorized requests, receipt, release, interception, dissemination, or discussion of CJI is serious and may result in criminal prosecution and discipline, including termination of employment.

Security Incidents

A **security incident** is a violation of the CJIS Security Policy that threatens the confidentiality, integrity, and availability of CJI. FDLE has written policies on reporting and responding to a security incident.

Security Incident Policy

FDLE has policies on the overall incident handling procedures, how the agency performs incident reporting, and incident management procedures in the event of a security incident. All FDLE members should be aware of the agency's policy regarding possible security incidents and the proper reporting procedures within the agency.

Incident Response Training

FDLE members with incident response responsibilities will be provided incident response training on how to properly prepare for, detect, contain, eradicate and recover from, a security incident.

Reporting Security Events

FDLE members must immediately report any suspected information security incidents. Suspected computer security incidents should be reported to the FDLE Local Agency Security Officer/ISM and to the FDLE Customer Support Center.

Acknowledgement of Completed Training and Member Responsibilities

with Unescorted Access to a Physically Secure Location

I have received, read and understand the Security and Privacy Training for individuals with unescorted access to a physically secure location. I understand that additional training will be required depending on my job duties and/or future access to Criminal Justice Information.

Member's Signature: _____

Date: _____

NOTE: Please submit the completed and signed form to the Office of Human Resources to be placed in the member's personnel file.