


POLICY 112.2	ACCESS TO CRIMINAL JUSTICE INFORMATION	
	REVISED: 5/98, 9/01, 09/11, 07/17, 12/18, 04/20, 09/21	RELATED POLICIES:
	CFA STANDARDS:	REVIEWED: AS NEEDED

A. PURPOSE

To ensure the proper documentation, protection, dissemination, and destruction of Criminal Justice Information, including FCIC/NCIC criminal history, Drivers and Vehicle Information Databases (DAVID), and personally identifiable information until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interests of public safety); purged, or destroyed in accordance with applicable records retention rules. This policy is intended to supplement the CJIS Security policy.

B. POLICY

It is the policy of the Fort Lauderdale Police Department to use criminal justice information, criminal histories, and personally identifiable information in accordance with CJIS Security Policy, Florida law, and Federal law. Criminal histories and criminal justice information shall only be used for authorized purposes. Persons violating this policy may be subject to administrative, civil, and/or criminal penalties.

C. DEFINITIONS

1. Criminal Justice Information (CJI) - Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.
2. Criminal Justice Information Services Division (FBI CJIS or CJIS) - The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.
3. Personally Identifiable Information (PII) – For the purposes of this policy, PII is information extracted from CJI 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.

D. PROCEDURE

1. CRIMINAL JUSTICE INFORMATION

The following procedure will be followed with respect to CJI:

- a. Information obtained from the CJI systems, must only be used for authorized criminal justice or noncriminal justice purposes as allowed by federal or state law. Personnel must follow all CJIS Security Policy, state and federal rules and regulations regarding CJI information. All personnel with access to CJI, shall receive the proper training within 90 days of hire or within 90 days from requiring the need to access such data.
- b. Dissemination of CJI containing criminal history is only permitted to authorized personnel, after validating the requester as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.
- c. Access to physical and digital media in all forms is restricted to authorized individuals only.
- d. Access to technology systems providing access to electronic media is for authorized individuals only and requires an account established according to policy 111.2 – D.
- e. Physical media (i.e. physical documents) shall only be stored for case file and validation purposes. When not in use the documents will be stored in a physically secure area in cabinets preventing viewing or access by visitors or unauthorized personnel. Documents will only be removed from filing cabinets when needed for operational purposes, and will not be left out where they can be viewed by visitors or unauthorized personnel.
- f. All servers containing CJI shall be maintained in a physically secured building inaccessible to non-authorized individuals. All entrances to the building shall have key card locks that are only accessible to Agency employees. Any servers outside of a physically secure location shall be encrypted with FIPS 140-2 certified encryption in order to secure the criminal justice data stored on them. Any documents shall be secured in the records division with access to only authorized personnel. When documents containing CJI are physically removed, the individual shall sign for the documents in the dissemination log maintained by the Records Unit.
- g. Physical media that contains CJI data that needs to be transported to another location shall be sealed in an envelope and driven directly to its final destination by authorized personnel only, where it will be handed over to an authorized individual. No additional stops are permitted during the transportation of CJI data.
- h. All computer screens will be oriented to prevent unauthorized viewing or “shoulder surfing”.

- i. CJI shall not be transmitted via email.
- j. CJI transmitted as a facsimile via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application, or service which implements email-like technology, shall meet the agency encryption requirements.
- k. CJI transported on digital media will adhere to the departments Digital Media Encryption Policy.
- l. Physical media (print-outs and other hardcopy physical media) that contains CJI data shall be disposed of according to the agency physical media destruction policy.

2. CRIMINAL HISTORY

The following procedure will be followed with respect to Criminal History:

- a. A criminal history log will be kept in the Records Teletype. This log will trace criminal history requests, their dissemination, and also function as a secondary dissemination log. The Special Investigations Division will also maintain a secondary dissemination log with other law enforcement agencies. These logs will be maintained for five (5) years as required by Florida Department of Law Enforcement and the Federal Bureau of Investigation guidelines.
- b. Any person accessing a criminal history will contact Records Teletype unit and provide the following information for placement in the criminal history log:
 - (1). Date of access to information;
 - (2). The name of the individual(s) whose criminal history was run;
 - (3). To whom the information was released;
 - (4). Who released the information;
 - (5). The State Identification (SID) and/or FBI numbers;
 - (6). The purpose for which the information was requested;
 - (7). Case number;

The information above will be used to validate the requester is an authorized recipient of the criminal history.

Any criminal histories released outside of the Department to another criminal justice jurisdiction must be logged on a Secondary Dissemination Log. Secondary dissemination logs will be maintained in the Criminal Investigation Division, Special Investigation Division, and Records Teletype unit.

- c. Once a criminal history has exhausted its administrative value, it will be disposed of according to State/City Records disposition requirements.

- d. Access to the Florida Department of Law Enforcement (FDLE) and Federal Bureau of Investigations (FBI) Criminal Justice Information Systems (CJIS) shall follow all guidelines as stated in the current FDLE CJIS Certification Security Policy.

3. PERSONALLY IDENTIFIABLE INFORMATION (PII)

The following procedure will be followed with respect to PII extracted from CJI:

- a. PII may be extracted from criminal justice information (CJI), but only for official purposes.
- b. PII will be protected in the same manner as CJI, as specified in D.1 above.
- c. Once PII has exhausted its administrative value, it will be disposed of according to the agency physical media destruction policy.

4. DRIVERS AND VEHICLE INFORMATION DATABASE (DAVID)

FLPD has access to DAVID in accordance with a Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV)

- a. Information obtained from DAVID may only be disclosed to persons to whom disclosure is authorized pursuant to Florida law (F.S. 119.0712(2)), the Driver's Privacy Protection Act (18 USC s. 2721-2725, and the Certification Program for Access to the Master Death File (15 CFR § 1110.
- b. Unauthorized disclosure of information from DAVID is a violation of this policy, and may subject the violator to criminal and civil sanctions.
- c. Department members are reminded that emergency contact information listed in DAVID is to be used only in emergency situations. These situations are identified as notifying the emergency contact of the death or serious injury of the subject due to an accident or natural disaster, or if the subject is believed to be missing.
- d. Accessing any individual's DAVID records for any other purpose other than an ongoing law enforcement incident, investigation, or other law enforcement purpose is strictly prohibited.
- e. The only people that have access to DAVID emergency contact information are Sergeants, Lieutenants, Traffic Homicide Investigators and Homicide Detectives.

5. THE ELECTRONIC LICENSE AND VEHICLE INFORMATION SYSTEM (ELVIS)

FLPD has access to ELVIS in accordance with a Memorandum of Understanding (MOU) with the Tallahassee Police Department (TPD)

- a. Only personnel who have been fully trained on the ELVIS system and who are currently CJIS certified will be permitted an ELVIS account.

- b. Department Personnel who are provided an ELVIS account may not provide and/or share their user name or password with anyone.
- c. All ELVIS users shall abide by all applicable local, state, and federal laws, rules and regulations, including, but not limited to, the rules and regulations of NCIC and FCIC with regard to the use of any device accessing CJI and/or ELVIS, and all terms and conditions contained in the Memorandum of Understanding entered into between the Tallahassee Police Department and the City of Fort Lauderdale for the use of ELVIS.
- d. ELVIS may only be accessed through Department (City) owned devices. Accessing ELVIS through any personally owned or public device is strictly prohibited.
- e. Access to the ELVIS system may be revoked if the user is found to be in violation of department rules and regulations for proper use.

6. PHYSICAL MEDIA DESTRUCTION

Physical media containing CJI or PII will be destroyed according to the following procedure:

- a. Shredding using the Fort Lauderdale Police Department issued micro cut shredders by agency personnel.