



Florida Fish and Wildlife Conservation Commission
Division of Law Enforcement

TITLE: CRIMINAL JUSTICE INFORMATION SERVICES

GENERAL ORDER	EFFECTIVE DATE	RESCINDS/AMENDS	Applicability
67	January 11, 2017	N/A	All Members

References

1 POLICY

A It is the policy of the Division of Law Enforcement to establish the Division's procedures for compliance with all aspects of the Criminal Justice Information Services (CJIS) Security Policy.

B Definitions:

- (1) **Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division (CJIS)** – The FBI division responsible for the collection, warehousing, and timely dissemination of relevant Criminal Justice Information (CJI) to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.
- (2) **Criminal Justice Information (CJI)** – Criminal Justice Information 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 including, but not limited to, biometric, identity history, biographic, property, and case/incident history data.
- (3) **User Agreement** – An executed agreement between the Florida Department of Law Enforcement (FDLE) and the Florida Fish and Wildlife Conservation Commission (FWC) stating the FWC will abide by all policies and procedures in the use of the CJI terminal and the information obtained from the CJI system.
- (4) **Physically Secure Location** – A facility, a law enforcement vehicle, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

2 RESPONSIBILITIES

A It is the responsibility of Fleet and Technical Services section to:

- (1) Ensure all members maintain current and appropriate CJIS certifications.
- (2) Ensure that members in the Office of Information Technology (OIT) and the Office of Inspector General (OIG) maintain current and appropriate CJIS certifications, as required.
- (3) Develop and implement training as required by CJIS.
- (4) Maintain a list of all members and their CJIS system authorization and level of certification.

B It is the responsibility of all members to:

- (1) Obtain and maintain the appropriate CJIS certification needed according to their job function.

3 PROCEDURES

A CJIS Certification

- (1) All members who have access to CJIS or CJI as part of their assigned duties or may access or overhear CJI shall have the appropriate certification from FDLE. Members who are required to maintain current CJIS certification and levels are:
 - (a) Sworn members (including Reserve Officers) – Limited Access Certification.
 - (b) Duty Officers, Duty Officer Supervisors and Non-Sworn Technology Services Staff that support the Regional Communications Centers – Full Access Certification.
 - (c) Non-Sworn members assigned to the Intelligence or Investigations sections that perform queries or background checks – Limited Access Certification.
 - (d) Non-Sworn members – CJIS Security Awareness Training.
- (2) New sworn members shall complete their Limited Access training prior to graduating from the FWC Academy.
- (3) Duty Officers and Duty Officer Supervisors shall complete the CJIS certification class within six months of employment. During the initial six-month period, the member may access the system utilizing a temporary access status and must be under the supervision of a certified user.
- (4) Non-Sworn employees shall complete the appropriate CJIS certification within six months of employment.
- (5) Members shall renew their CJIS certification every two years.

B Security

- (1) Members shall take precautions to ensure that CJI is secure at all times. Before information is released to the public or other agency personnel, the member shall ensure that the receiving entity is permitted by CJIS standards to receive the information.
- (2) Only agency owned and managed computers shall be authorized to access, process, store or transmit CJI unless FWC OIT has approved specific terms and conditions for access or use from personal devices.
- (3) CJI shall not be stored on personally owned or unencrypted electronic physical media such as USB thumb drives, removable memory cards, etc. All electronic storage of CJI should be done on a member's issued computer or the member's "U" drive. For instructions on properly encrypting electronic physical media please see the Technology Services Section Share Point site.
- (4) Any CJI that is printed shall be stored in a secure location (i.e. locked patrol vehicle, locked filing cabinet, desk drawer, or office). When the printed document is no longer needed, it shall be shredded. CJI documents shall not be maintained as part of a case file.
- (5) Members shall escort visitors that are not CJIS certified to their work areas to prevent unauthorized view or access to CJI. Members in that work area shall be made aware that there is an uncertified visitor present and to operate accordingly to maintain the confidentiality of the system.

C Uses

- (1) Members shall not use CJI for any non-criminal justice purposes without approval from the Division Director.

4 FORMS

FORM NUMBER	FORM TITLE
N/A	N/A