
	Florida State University Police Department	
CJIS Compliance		
Revision Effective Date: 09/05/17	General Order 1107	Attachments: None
Rescinds/Amends: 33F (12/19/16)	Distribution: Department Wide	CFA Reference: None
	Pages: 7	

POLICY

The purpose of this general order is to establish guidelines and regulations governing access and security of the Criminal Justice Information System (CJIS). It is the policy of FSUPD to secure PII and use and maintain CJIS resources and applications in accordance with the Criminal Justice Information Services Security Policy, and to take appropriate action when violations occur.

PROCEDURES

A. PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII is information 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.

PII may be extracted from criminal justice information (CJI), but only for the official purposes only. Once PII has been used, personnel must dispose of all information properly. PII must not be disseminated to other agencies.

B. INFORMATION EXCHANGE

Dissemination of information should only be given to those agencies with an information exchange agreement. Personnel must identify the agencies and personnel requesting information.

All Disseminated CJI shall be documented in the dissemination log including: date, subject's name, SID or FBI number, requestor, requestor agency, operator, reason disseminated, and purpose code.

C. INFORMATION HANDLING

Information obtained from the CJJ systems, must only be used for criminal justice purposes. Personnel must follow all CJIS Security Policy, state and federal rules and regulations regarding CJJ information. All personnel with access to CJJ, audio as well as visual, shall receive the proper training within 30 days of hire. CJJ or PII will not be transmitted via email unless encrypted. All information outlined in the information exchange and disposal of physical media shall be followed as well. These procedures shall include all inquiries for both criminal justice and non-criminal justice purposes.

D. INCIDENT RESPONSE

Should an incidence occur involving any device (workstations, smart phones, laptops, tablets, etc.) that is on the Florida State University Police Department network, the LASO shall be contacted immediately. If it is deemed by the LASO to be a security breach of confidential information, a Security Incident Response Form will be filled out and submitted to FDLE ISO at fdlecjisiso@flcjin.net.

The LASO will identify the security breach by conducting the following:

1. Confirm the discovery of a compromised resource(s).
2. Evaluate the security incident.
3. Evaluate the security incident.
4. Identify the system(s) of information affected.
5. Review all preliminary details
6. Characterize the impact on the agency as: minimal, serious, or critical.
7. Determine where and how the breach occurred.
 - a. Identify the source of compromise and the time frame involved. Review the network to identify all compromised or affected systems.
8. Examine appropriate system and audit logs for further irregularities
 - a. Document all internet protocol (IP) addresses, operating systems, domain system names and other pertinent system information.
9. Initiate measures to contain and control the incident to prevent further unauthorized access.
10. Document actions throughout the process from initial detection to final resolution.

E. ACCOUNT MANAGEMENT

The management of CJJ system accounts shall be conducted by Information Technology personnel at the direction of the LASO in accordance with all policies and CJIS Security Policy requirements. New employee personnel will gain access to all systems upon start date, but will lose access to CJJ systems if training courses are not completed and passed within 30 days. All user accounts of retired, terminated or otherwise former and non-working employees shall be disabled and revoked

immediately or as soon as practicable. User accounts suspected of compromise shall be immediately disabled upon first discovery of compromise. Logs of access privilege changes shall be maintained for a minimum of one year and document the validation process.

The biennial security awareness training must be completed by all authorized personnel. Any employee who has not completed the required training will be removed from the CJIS System by the department TAC until the training has been completed.

F. SYSTEM ACCESS CONTROL

Access to all CJIS systems will be granted by the agency's LASO. Once access is granted, the Information Technology (IT) Department will control access. Multiple concurrent sessions are allowed for as some individuals that have more than one computer at their workstation. (i.e. Communication Officers and FSUPD IT Staff). To ensure accountability, users are prohibited from sharing user login information or from working at a computer logged into by another user. All other purposes must be approved by the LASO.

G. REMOTE ACCESS

Remote access shall only be used for official use only. This includes those on duty patrol officers remoting into the agency's network using a VPN tunnel. IT personnel may remote access into the agency's network only for emergency purposes. Vendor companies may be granted access to the agency's network only if the CJIS Security Awareness Training has been completed and certification is current, the necessary Fingerprint Based Criminal Background Check has been performed, and the Security Addendum has been signed.

H. PERSONALLY OWNED DEVICES

Personally owned devices are not allowed to access the CJIS network. A device that is not owned by Florida State University Police Department, shall not process, store, access or transmit CJIS.

I. AUTHENTICATION STRATEGY

If personnel are on the agency's network, a user name and password is required. All passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User name.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.

6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

J. AUTHENTICATION MANAGEMENT

Authenticators will be assigned to personnel during training or upon reassignment. Any lost, compromised, or damaged authenticators should be reported to the IT department immediately. Authenticators shall be deactivated immediately if personnel is terminated, retired, or has been reassigned.

K. AUDIT LOGS

Florida State University maintains logs of all systems having access to CJI data. Logs will be maintained for at least one (1) years' time, and will be reviewed on a weekly basis.

L. MEDIA PROTECTION

Media in all forms shall be protected at all times. Electronic media (i.e. hard drives, disks, flash drives, etc.) shall be behind locked doors at all times with access granted only to authorized personnel only.

Physical media (i.e. physical documents) shall only be stored for case file and validation purposes. CJI stored will be placed in locked filing cabinets behind locked doors. Only authorized personnel will be granted access. All other forms of CJI shall be shredded when not in use.

M. ELECTRONIC MEDIA SANITIZATION AND DISPOSAL

All electronic media no longer in use will be sanitized. The device will be overwritten three times by using Acronis Drive Cleanser. Once overwritten the device shall be stored behind locked door until disposed of in the University's Hard Disk shredder.

N. DISPOSAL OF PHYSICAL MEDIA

All physical media, when no longer in use, will be disposed of by agency's shredder. The shredder purchased shall be a cross-cutter shredder.

O. PHYSICAL PROTECTION

The agency's hardware, software, and media containing confidential information will be stored behind locked doors. Only authorized personnel with a "need to know" or "right to know" based on job duties will have access.

The agency shall control physical access by authenticating all visitors before authorizing escorted access to the physically secure location. The agency shall escort visitors at all times and monitor visitor activity.

P. ENCRYPTION

When CJJ is transmitted outside the physically secure location, the agency will encrypt all data with at least 128-bit encryption. The encryption mechanism shall meet FIPS 140-2 requirements and certificate shall be kept on file at all times.

At the moment the agency does not utilize PKI.

Q. VOICE OVER INTERNET PROTOCOL

The agency does utilize a Voice over Internet Protocol (VoIP) for the telephone system. It is located on its own separate network.

No CJJ shall be spoken over the VoIP line.

R. PATCH MANAGEMENT

The agency's IT department shall review all security relevant patches, service packs, and hot fixes from the vendors. Once reviewed, the patches will be fixed promptly.

S. SECURITY ALERTS AND ADVISORIES

Security alerts and advisories will be subscribed by the IT Department. IT personnel shall evaluate each security alert to determine its urgency and relevance to the agency. Then promptly develop a plan of action to respond to any changes in threats or vulnerabilities exposed by those alerts and notify the proper agency personnel.

T. WIRELESS ACCESS RESTRICTIONS

Florida State University Police Department does not provide wireless access within the department's network. The available wireless access is provided by the University and is on its own separate network apart from the Police department. Staff is provided access to FSUSecure with their employment. Guests are provided access to FSUGuest and must sign up for a 24 hour pass.

U. BLUETOOTH

Bluetooth will only be used for official business purposes. The purposes include the agency's Rapid IDs, printers, and wireless mice. All other Bluetooth devices shall be approved by the agency's IT department.

V. PERSONNEL SANCTIONS

All FSUPD personnel shall adhere to all policies. Failure to do so will require review by the agency head. Once reviewed, personnel may receive disciplinary actions, up to and including termination and/or criminal prosecution.

Glossary

Agency – The Florida State University Police Department.

Biennial – An event occurring once every two years.

Criminal Justice Information (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 including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Network (CJNet) - CJNet is a secure Intranet designed for use by the Florida criminal justice community.

LASO (Local Agency Security Officer) - Every agency that accesses FCIC/NCIC and/or CJNet must designate a LASO to ensure compliance with the FBI CJIS Security Policy and any other applicable security requirements. The LASO should be knowledgeable about technical aspects of the agency network or be able to confirm information through local technical support. (The LASO for FSUPD is the IT Manager)

Personally Identifiable Information (PII) - (as defined by the CJIS Security Policy), information 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. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII.

Remote Access- Any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g. the Internet).

Index

CJIS

CJI

Criminal Justice Information

Criminal Justice Information Services

LASO

Local Agency Security Officer

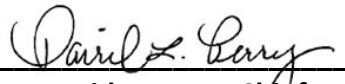
Personally Identifiable Information

PII

MTC 09/05/17 Filed: General Order 1107

Title: **CJIS Compliance**

Approved:


David L. Perry, Chief

Effective Date: 09/05/17