PERSONALLY IDENTIFIABLE INFORMATION POLICY

Purpose

The purpose of this policy is to define standards and procedures for ensuring appropriate controls are applied when handling Personally Identifiable Information (PII) extracted from CJI. Hereinafter the word Agency as capitalized refers to the ***ENTITY***, a criminal justice agency authorized by statute and agreement to handle CJI.

Scope

This procedure shall apply to all Agency personnel. It addresses Personally Identifiable Information (PII) extracted from CJI and any PII extracted from other entities (i.e. driver license information, vehicle registration information, etc.).

Discussion

The overriding goal of this policy is to ensure that personnel that collects PII at the Agency does so in compliance with state and federal regulations and best practices for information security in law enforcement.

Definitions

A. **Criminal Justice Information (CJI)** – As defined in Policy 4.1 of the CJIS Security Policy. In general, it is any information including, but not limited to, biometric, identity history, biographic, property, and case/incident history that has not been officially released to the public or otherwise authorized for release by court order.

B. **CSA** – The criminal justice agency responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels.

C. **FIPS** – FIPS (Federal Information Processing Standards) are a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

D. **FIPS 140-2** – Defined as a federal mobile security certification.

E. **NIST** – NIST is the National Institute of Standards and Technology, a unit of the U.S. Commerce Department. NIST promotes and maintains measurement standards. It also has

active programs for encouraging and assisting industry and science to develop and use these standards.

F. **Personally Identifiable Information (PII)** – Defined as information about a person that contains some unique identifier, including but not limited to name or Social Security Number, from which the identity of the person can be determined.

Procedure

Policy and Appropriate Use

A. **Collection**
PII shall be collected only when the Agency has the legal authority to do so and the PII is necessary to the conduct of official duties.

B. **Limit Use**
Access PII only when the information is needed in the conduct of your official duties. PII is to be utilized for official purposes only. PII shall not be utilized for personal reasons.

C. **Limit proliferation**
Do not create unnecessary or duplicative collections of PII. If you need to create duplicate copies of documents containing PII to perform your duties then delete or destroy them when they are no longer needed. Unauthorized replication, especially for personal use, may constitute a violation of policy. When you need to print, copy, or extract PII from documents, target only the PII that is required for the task at hand.

D. **Retention**
The retention of PII extracted from any Agency system shall not extend beyond the State retention policies for that data in the Agency system.

E. **Security**
1. The following measures shall be taken to ensure the protection of PII:
    a. Any mobile computer, mobile computing device or removable storage media that processes, stores, or transmits electronic records containing PII shall store and transmit that data encrypted. That encryption shall conform to standards specified in the CJI Information Handling section (MINIMALLY NIST-CERTIFIED, FIPS 140-2 OR CURRENT). User authentication providing access to said data shall be via an authorized advanced authentication mechanism or passwords as specified in the

Information Security Policy. Approved software for file and folder encryption is available from the Technical Services Unit.

b. Storage of PII shall be restricted to Agency owned devices. PII shall not be stored or transmitted via personally owned devices including but not limited to computers, cellphones, flash drives, CDs, and DVDs.
c. Do not take PII home or to any unsecured worksite in either paper or electronic form unless appropriately secured. PII in electronic form must be encrypted as specified above.
d. When e-mailing PII to any recipient not covered by an Agency Agreement or transmitted via an unsecured network then PII must be sent via an encrypted attachment with the password provided separately (e.g. by phone or in person).
e. Do not leave PII unattended in any unsecured space where it might be accessed by unauthorized persons.
f. Store PII in shared access computer drives ("shared folders") only if access to those folders is restricted to those with a need to know by access permissions.
g. Physically secure PII when in transit. Do not mail or courier PII on media unless the data is encrypted.
h. Protect PII data during all stages of life cycle. Do not discard or provide any vendor for maintenance media holding PII. Do not place laptops or removable media in checked baggage. Do not leave them in an unsecured car overnight or unsecured in plain sight in public places.
i. If you are sent unsecured PII you still must secure it once you receive it.
j. Adhere to all provisions of Information Security Policy.

F. **Misuse**

Any suspected violation of the Personally Identifiable Information (PII) section will immediately be investigated. Misuse of PII information involving violation of CJIS Security Policy must be reported to the CSA.

G. **Incident Response**

All information security events including those involving personally identifiable information shall be promptly reported in accordance with the Information Security Incident Response Policy. The report shall include date and time of occurrence, PII data compromised, known and suspected unauthorized recipients, and whether the data was encrypted as required above. When possible an Incident Response Form should be completed and sent to the Technical Services Unit.

H. All requirements of FBI Security Policy relevant to PII shall be included by reference.

I. All requirements of the Agency CJI Information Handling Policy are included by reference.

Policy Noncompliance

Failure to comply with the Personally Identifiable Information Policy may, at the full direction of the ***Administrator***, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.