**AGENCY NAME**

**Title: Information Exchange**

**Number: XXX Effective: 6/01/16**

**Amends: XXX**

**Distribution: All**

**Standards**:

All information shared through communication mediums shall be protected with appropriate security safeguards. There must be agreements established between parties that allow for the exchange of criminal justice information along with agreed upon security standards for the release and receipt of such information.

|  |
| --- |
| **Scope** |

This procedure shall apply to all Agency personnel.

|  |
| --- |
| **Discussion** |

The overriding goal of this policy is to comply with the CJIS Security Policy requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of AGENCY NAME. The Agency shall adhere, at a minimum, to the CJIS Security Policy. While the Agency may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

|  |
| --- |
| **Procedures** |

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. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

**1. Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

**2. Identity History Data**—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

**3. Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

**4. Property Data**—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

**5. Case/Incident History**—information about the history of criminal incidents.

The Agency will put forth formal agreements with other agencies prior to exchanging criminal justice information as well as the use of secondary dissemination.

The Agency allows for criminal justice information to be shared with \_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_, and \_\_\_\_\_\_\_\_\_\_. This exchange is allowed only via hard copy and \_\_\_\_\_\_\_\_\_\_\_\_\_ applications.

The Agency will verify the receiver of the information by having a list of current authorized individuals that are allowed access to certain information. The Agency will validate that the receiver is on the list and document the information given as well as the identity of the requestor in a secondary dissemination log.

POLICY VIOLATION: Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with the Agency. Sanctions against staff that violate information systems and or security policies may include formal disciplinary action up to and including termination based on offense severity.