**AGENCY NAME**

**Title: Information Handling**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Criminal justice information must be handled securely to avoid unauthorized disclosure, alteration or misuse. The purpose of this policy is to document how the Agency handles and stores criminal justice 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** |

The Agency utilizes servers for storage of criminal justice information. The servers are kept in a physically secured building inaccessible to non-authorized individuals. The doors have key card locks that are only accessible to Agency employees. The servers are encrypted with FIPS 140-2 certified encryption in order to secure the criminal justice data stored on them.

Physical information, such as reports that contain criminal justice information is stored in the dispatch room that is only accessible to Agency personnel. The documents are stored in a locked filing cabinet and are only removed when needed for operational purposes. When removed, the information is kept by an authorized individual and then returned. The removal is documented in a log.

Any information that must leave the facility for transport will be done so only by authorized personnel and only for operational purposes.

All computers within the facility are turned away from view to prevent unintentional viewing or shoulder surfing.

All emails that are sent with criminal justice information are sent via CJNET email. This ensures that the information is encrypted from end to end.

Any information that is shared with another agency will only be done after an information exchange agreement has been put in place. Any information that is shared with another agency is documented in a secondary dissemination log and maintained for four years.

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.