**AGENCY NAME**

**Title: Physical Protection**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

The purpose of this policy is to provide guidance for all agency personnel, support personnel and private contractors and vendors for the physical, logical and electronic protection of 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** |

Physically Secure Location:

The Agency is deemed a physically secure location. Only authorized personnel have access to the building. The building is equipped with badge swipe access for Agency personnel. Visitors must sign in at the front desk and produce identification. The Agency does not allow unescorted access by any non-agency member. When escorted into the building, visitors will wear a visitors badge and be accompanied by an authorized Agency member. All computer screens will be turned away from public view. All physical media containing CJI will be locked in filing cabinet in a locked office. Only authorized personnel will have a key to the cabinet. All computer components will be locked in the secure server room. Only IT will access to the server room. All vendors and contractors will undergo fingerprint based records checks under the Agency ORI and will complete appropriate security awareness training. Any transportation of CJI will be done so securely. Only authorized personnel can transport CJI. It will physically be with the personnel or, if electronic, will be done so encrypted. All Agency computers will be equipped with boundary protection tools and spam and spy ware to avoid any intrusion attacks.

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.