**AGENCY NAME**

**Title: Media Protection**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

The purpose of this policy is outline how media is protected in a secure manner by authorized individuals of the Agency.

|  |
| --- |
| **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** |

Digital and physical media is restricted to authorized individuals. Only those users of the Agency who have undergone a fingerprint based record check and have appropriate security awareness training will be allowed to handle criminal justice information in any form.

Handling physical media- The Agency will ensure that only authorized individuals will be granted access to media containing criminal justice information. The media will be stored within the physically secure building and kept behind locked doors and locked cabinets.

Any computer that accesses criminal justice information within the facility will have a screen cover to ensure that information is not viewable by any unauthorized individual.

Any media that is transported outside the physically secure location will be kept in a sealed envelope with evidence tape to ensure that the chain of custody is kept. When the media is released to another user, the user will document the transaction in a secondary dissemination log for validation purposes.

At no time will the physical media be released to an unauthorized person or left without proper documentation.

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.