**AGENCY NAME**

**Title: Electronic Media Sanitization and Disposal**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Electronic media that has reached the end of its lifecycle must be sanitized and disposed of to ensure that criminal justice information is not viewed or accessed by unauthorized individuals. Electronic media is defined as any electronic storage device that is used to record information, including, but not limited to: hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as USB drives.

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

All electronic media must be properly sanitized before being transferred from the custody of the Agency. The proper method of sanitization depends on the type of media and the intended disposition of the media.

Hard Drives: The Agency will overwrite the hard drive utilizing a three pass wipe. This will ensure that the data on the drive is overwritten with patterns of binary ones and zeros. The sanitization of the hard drive is not complete until the third wipe passes and a verification pass is complete.

Destruction of the hard drive will incorporate drilling into the drive. This will be carried out or witnessed by authorized Agency personnel.

USB drives, floppy disks, rewritable CD-ROMS, zip disks, videotapes and audiotapes will be erased if able and then destroyed by drilling or smashing, witnessed or carried out by authorized Agency personnel.

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.