**AGENCY NAME**

**Title: Personally Owned Devices**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Personally owned devices include cell phones, tablets or any other device that is owned and maintained by the user, not 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** |

The Agency does not allow personally owned devices to access, store or transmit criminal justice information. Under no circumstance are users allowed to connect their personal device to the Agency network or any Agency owned devices, applications or systems.

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.