**AGENCY NAME**

**Title: Bluetooth Technologies**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Bluetooth technology is utilized as the open standard for short-range radio frequency communication. This policy provides the minimum baseline standard for connecting Bluetooth enabled devices to the Agency owned devices. The Agency utilizes Bluetooth technologies for operational processes only.

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

Bluetooth technology, while not as secure as other forms of wireless technology is utilized for operational needs within the Agency. Currently, the Agency utilizes Bluetooth technology with the Rapid ID device. The device relies on Bluetooth due to the ability of the technology to operate in noisy environments by moving from frequency to frequency. By doing this, the device avoids getting interference from other signals as it transmits or receives the identifying information.

The user must only use Agency owned Bluetooth devices to pair with criminal justice information systems. Currently, the user may only use the Rapid ID device for Bluetooth Technology. The Agency maintains these devices and ensures that they meet the minimum requirements of Bluetooth specifications. All other Bluetooth devices are not to be utilized to pair with Agency systems, networks, and hardware.

* The Agency is responsible for maintaining an encrypted security mode between the device and the pair.
* The Bluetooth device must be in hidden mode to ensure that other individuals cannot connect to it.
* The user should only activate Bluetooth when it is needed to perform an identification check
* The Agency must ensure the firmware is up-to-date and that all patches are current

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.