**AGENCY NAME**

**Title: Wireless Restrictions and Review of Wi-Fi Logs**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Agency Name has implemented a wireless network for ease of daily operations. The use of the wireless network is for Agency information and systems only and should be utilized as such. The purpose of this policy is to provide the requirements for utilizing criminal justice information system(s) with wireless access.

|  |
| --- |
| **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 utilizes wireless access for the ability access the Agency information system. Agency personnel are only permitted to use the Agency wireless network for Agency business. Personnel may only access the network with Agency owned equipment. The IT department will authorize individual users to utilize the network by giving them an agency owned mobile device terminal. The IT department will monitor all connections and audit logs associated with the devices as well as the systems and applications that the device accesses. IT will review these audit logs on a monthly basis or more frequently if there is an increased risk to agency information or systems.

Agency personnel are not allowed to access Agency systems on any public wireless network. The access to the information system is only allowed for job-related functions. All personal use is prohibited. Users are not permitted to attempt to add, remove or modify any hardware, software, network devices or other information systems in place within the Agency.

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.