**AGENCY NAME**

**Title: Voice over Internet Protocol (VoIP)**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Voice over Internet Protocol (VoIP) is the routing of voice conversations over a packet switched network as opposed to the traditional circuit-switched telephone network. Voice and data convergence introduces many security issues that must be addressed prior to deployment and use of VoIP technology. The purpose of this policy is to define standards and procedures for the implementation of VoIP telephone systems as well as lay out restrictions in regards to criminal justice information.

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

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

To ensure the secure environment of the VoIP system, the Agency will enable the underlying data network is configured to host efficient bandwidth and reliability. The VoIP server will be dedicated only for applications required for VoIP operations.

IT will ensure that software patches for the VoIP system and servers originate from the system manufacturer and are applied in accordance with the manufacturer’s instructions prior to implementing the patches.

Security:

The Agency will ensure all critical VoIP network and server components are located in the physically secured area and that only authorized personnel have access to them. This will limit physical access to the VoIP network segment.

The Agency will ensure that the default administrative password on the IP phones and VoIP switches are changed prior to implementation.

The Agency will utilize Virtual Local Area Network technology to segment VoIP traffic from the data traffic. The Agency will ensure that the VoIP system is not on the same VLAN as the Agency’s information network.

The Agency will use IPsec for all remote management and auditing access of the VoIP system.

The Agency has enabled a VoIP-ready firewall designed for VoIP protocols to aid in securing the system.

Agency members will avoid openly discussing criminal justice information over the VoIP phone lines unless there is an immediate need such as a safety concern.

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.