**AGENCY NAME**

**Title: Incident Response Including Mobile Devices**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

The purpose of this policy is to detail the actions of users for reporting or responding to security incidents involving **AGENCY NAME** to ensure effective and consistent reporting and handling of events.

|  |
| --- |
| **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 users are responsible for reporting known or suspected information or information technology security incidents. All incidents must be reported immediately to the Agency LASO. The LASO will inform a member of IT and document the incident.

If a suspected incident occurs on a user’s mobile device, the user shall not turn off the device. The user will leave the device on and report the incident. A member of IT will look over the device and determine if the incident is contained to the one device or if it is within the Agency system.

The agency will employ Kaspersky Antivirus on all desktop and laptop devices and will ensure that the antivirus software is up-to-date.

Incident response will be managed based on the level of severity of the incident. The level is a measure of its impact or threat on the operation or integrity of the Agency and its’ information. High Level (potential to impact the network or criminal justice information) Medium Level (potential to impact one system or non-critical system) Low Level (has little or no risk of infecting a criminal justice system).

If the level is moved to High, the LASO will notify FDLE immediately.

All Security Incidents will be documented on a security incident reporting form, kept by the LASO and retained for no less than a three year period.

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.