**AGENCY NAME**

**Title: Patch Management**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

This policy describes the Agency’s requirements for maintaining up-to-date operating system security patches on all Agency owned and managed workstations and servers.

|  |
| --- |
| **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 workstations, mobile devices and servers owned by the Agency must have up-to-date operating system security patches installed in order to protect the device and network from known vulnerabilities.

Workstations, desktops and laptops have automatic updates enabled for the operating system patches. Current Agency servers have the minimum baseline requirements that define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Agency’s data and network.

IT will manage the patching needs for the servers on the network. In addition, they will manage the patching needs for all workstations on the network. IT will routinely assess the compliance of the patching policy and will provide guidance to all personnel of any security and patch management issues. IT also approves monthly and emergency patch deployments if necessary.

IT will monitor and report the outcome of each patching cycle to the Agency LASO. This will enable the LASO to assess the current level of risk.

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.