**AGENCY NAME**

**Title: System Access Control**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Access control policies are high-level requirements that specify how access to the information system(s) are managed and who may access the information under what circumstance. The purpose of this policy is to define standards and procedures for multiple concurrent sessions within the Agency information system(s).

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

Access to Agency information system(s) are based on a user’s right to know, authority, and user group.

The Agency does not allow multiple concurrent sessions within the network.

.

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.