**AGENCY NAME**

**Title: Remote Access**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

The Agency utilizes remote access to communicate with information systems through an external, non-agency-controlled network. The purpose of this policy is to outline acceptable methods of remote access and the security in place to keep the information system(s) secure.

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

It is the responsibility of Agency employees, contractors and vendors with remote access privileges to the Agency network to ensure that the connection is secure. All remote access to the Agency information systems must be done through the Agency’s VPN tunnel. The tunnel will be verified as FIPS 140-2 certified. Those personnel accessing the VPN must use advanced authentication as a secondary form of authentication in order to access the network. All access for contractors and vendors performing IT work will be done utilizing encrypted remote access. The Agency authorizes Bomgar Remote Access for this, which is FIPS 140-2 certified. IT will monitor and control all remote access to the Agency systems. For Virtual escorting, the Agency allows this for compelling operational needs. In these cases, IT will monitor the session, be familiar with the system where work is being performed as well as have the ability to end the session at any time. IT must verify the person gaining access prior to allowing the session. This will be done through advanced authentication (PIN).

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.