**AGENCY NAME**

**Title: Authenticator Management**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

Each user who is authorized to access, store, process, administer and maintain the criminal justice systems and applications, and/or transmit criminal justice information must be uniquely identified. The purpose of this policy is to define standards and procedures for authenticator management.

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

Each user that accesses criminal justice information must be uniquely identified prior to being given access to the system and information. The Agency uses standard authenticators (passwords) as well as advanced authenticators (grid card) for accessing criminal justice information in a secure manner.

A temporary standard authenticator is given to the user via the LASO during the first active session the user has. The user then creates a new password outlined in the authentication strategy policy.

Advanced authenticators are given to users prior to gaining access to criminal justice information outside of the physically secure location. The Agency utilizes grid cards for Advanced Authentication. The LASO will set up individual user access to retrieve the grid card.

Grid Card Care:

* The user must maintain possession of their grid card at all times
* The grid card must be stored in a secured area, out of sight from others
* The user shall not share their grid card or loan the card to other users
* If the user loses their grid card, the user must immediately report the loss to the LASO
* If the user believes their grid card has been compromised, the user must report the issue to the LASO
* The user must renew their grid card at a minimum of once per year

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.