**AGENCY NAME POLICE DEPARTMENT**

**GENERAL ORDER**

**Purpose**

**Title: Authentication Strategy (Passwords)**

**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 the administration of user and system passwords.

**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**

This Password Policy applies to all information systems and applications that contain criminal justice information or services. This includes, but is not limited to:

* Mainframes, servers and other devices that provide centralized computing capabilities
* SAN, NAS and other devices that provide centralized storage capabilities.
* Agency issued desktops, laptops, or any other device that provides distributed computing capabilities.
* Routers, switches and other devices that provide network capabilities.
* Firewalls and other devices that provide dedicated security capabilities.
* Windows Domain Accounts, Agency e-mail accounts, SmartCop application accounts as well as any other criminal justice information system or service.

The Agency LASO will ensure each account is set up with a temporary password. When the user initiates a first time log-on, the temporary password will be entered and the user will be prompted to create a new password.

The Agency dictates that each password and User-ID be unique and not be shared with any other individual. Users are forbidden to share their unique password or write it down. All passwords must be memorized.

**Password Requirements:**

The Agency utilizes individual passwords for gaining access to criminal justice information and systems. As such, all passwords must follow the requirements outlined below:

* Agency user passwords must contain at least 8 characters
* The user may not use a proper name or a dictionary word as a password
* The user cannot use their user-id as the password
* The password is set to expire every 90 days
* The user cannot reuse the previous 10 passwords
* The password cannot be transmitted in the clear outside the secure location
* The password will not be displayed when entered

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.