**AGENCY NAME**

**Purpose**

**Title: Account Management**

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

**Amends: XXX**

**Distribution: All**

**Standards**:

The purpose of this policy is to define standards and procedures for the administration and management of user accounts for authorized users of the AGENCY NAME. Hereinafter, the word Agency as capitalized refers to the AGENCY NAME, a non-criminal justice agency authorized by statute and agreement to handle criminal justice information.

**Scope**

This procedure shall apply to all AGENCY NAME 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**

The Agency LASO is the point of contact for all accounts. The LASO shall manage information system accounts to include establishing, activating, modifying, reviewing, disabling, and removing user accounts on all Criminal Justice Information Systems.

**Account Creation:**

1. Upon completion of appropriate state and national fingerprint-based records check, the Agency will notify the LASO and provide the following information regarding the user:
2. Applicant full name
3. Applicant date of birth
4. Applicant social security number
5. Applicant start date
6. Applicant assigned MDT (laptop)
7. Applicant system(s) access
8. Applicant system(s) permissions
9. The LASO will create and establish a Windows Domain account for the applicant. Each account is uniquely identified by a user name derived from the user’s last name followed by the first three letters of the applicants’ first name. All accounts are created to ensure a unique username for every individual.
10. The Domain account will be assigned a temporary password and will be set up to require the user to create a new password upon activating the first session. The password for the account must adhere to the Agency password requirements outlined in the Authentication Strategy Policy.
11. The LASO will establish an account for the \_\_\_\_\_\_\_\_\_\_\_\_\_ system for the user utilizing the same username requirements.
12. The LASO will identify the level of authority for the user for each application.
13. Administrator
14. User
15. The LASO will provide the initial credentials and temporary password to the users’ supervisor.
16. Upon completion of paperwork, the user will be issued Agency equipment delegated to the users’ position within the Agency. Equipment includes, but is not limited to, Agency laptop, MiFi device for wireless access, keys, identification badge and authentication token (grid card) and will sign a receipt all items. Subsequent equipment changes, deletions, enhancements will be documented via Agency equipment receipt form and approved through Agency chain of command.
17. The LASO will meet with the new user upon starting to ensure proper access to each information system is granted.

**Account Modification**

In the event of promotion, demotion, suspension, leave or voluntary or involuntary termination, the supervisor will immediately notify the LASO of the change of status to ensure appropriate access changes are made to systems and applications.

1. Promotion/Demotion- Supervisor will notify LASO of the change of status and change of authority level.

* The LASO will update all systems and applications as necessary to evolve with the current status of employment and will document these changes in the active directory.

1. Suspension/Leave- Supervisor will notify LASO of the temporary change to the users’ account.

* The LASO will temporarily deactivate the account on each system and application.
* The Supervisor will collect all agency equipment from the user and document the transaction.
* Upon reinstatement, the supervisor will notify the LASO and return all agency equipment to the user.
* The LASO will reactivate the user accounts on all systems and applications.
* The user will verify that the accounts are active and sign an equipment receipt.

**Account Termination**

* Upon termination from the Agency, whether voluntary or involuntary, the supervisor will inform the LASO of the employment change.
* The LASO will disable all accounts on all information systems and applications.
* The LASO will place the user in the Disabled User Organizational Unit within Active Directory, remove all access of controls from the user, disable Agency e-mail account, and remove remote access ability and all permissions.
* The supervisor will collect all Agency equipment and have the user sign the equipment receipt.

**Account Validation**

* The LASO will validate Agency User Accounts and Access Privilege Levels quarterly.
* The LASO will document the date and time of the validation on the Agency Validation Form.
* The LASO will verify that all active accounts are current and up-to-date.
* Any changes made by the LASO involving an account will be documented.

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.