<INSERT AGENCY NAME(S)>

CJIS User Account Validation Policy

|  |
| --- |
| *The purpose of this template is to assist your agency in creating its own procedures. These are the minimum topics that must be covered:*  *\*\*\*\*\*This document can cover multiple agencies supported by the same IT team\*\*\*\*\**   1. *The items below in red must be specific and reflect your agency’s current practices.* 2. *Remove any items that are not applicable to your agency.* 3. *Formalize with the date and your agency name.* 4. *Remove the red box once the procedure is updated and completed.*   *If your procedure does not reflect the actual practice at your agency, then you will be found out of compliance.*  *ACCESS Section revised October 2022* |

**Purpose**

All accounts shall be reviewed at least every six months (CJIS Security Policy requires annual review, the FBI recommends every six months) by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.

All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The TAC must disable all new accounts that have not been accessed within 30 days of creation.  Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual’s account(s) to the new office (CJA).

The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC).

The TAC shall:

* Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
* Periodically review existing accounts for validity (at least once every 6 months), and
* Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.