User Account – Access Validation Policy Sample

(Required Written Policy)

1.0 Purpose

To establish requirements for user accounts and access validation for all criminal justice networks to ensure the security of system access and accountability.

2.0 Scope

All accounts shall be reviewed annually by the [*terminal agency coordinator (TAC)/local agency security officer (LASO)/System Administrator 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/LASO/ System Administrator or his/her designee*] may also conduct periodic reviews.

3.0 Policy

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/LASO/ System Administrator or his/her designee]* should 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 should have a manager-approved request from the designated account administrator or assistant.)

The [*TAC/LASO/ System Administrator or his/her designee]* 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/LASO/ System Administrator or his/her designee]* will transfer the individual's account(s) to the new office (CJA).

The [*TAC/LASO/ System Administrator or his/her designee]* 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 [*TAC/LASO/ System Administrator or his/her designee]*.

The [*TAC/LASO/ System Administrator or his/her designee]* shall:

- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
- Periodically review existing accounts for validity, and

- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

4.0 Penalties

Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, and termination of employment.