



MYRTLE BEACH POLICE DEPARTMENT ADMINISTRATION REGULATIONS AND OPERATING PROCEDURES

Subject: Account Management and Validation

Number: 144

Effective Date: October 26, 2023

Revised Date:

Rescinds:

Dated:

Approved By:

I. DISCUSSION:

Computer accounts are the means used to grant access to Myrtle Beach Police Department's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for Myrtle Beach Police Department usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

II. PURPOSE:

The purpose of this policy is to establish a standard for the creation, administration, use, validation and removal of accounts that facilitate access to information and technology resources at Myrtle Beach Police Department.

III. PROCEDURE:

A. Accounts

- i. All accounts created must have an associated written request and signed management approval that is appropriate for the Myrtle Beach Police Department.
- ii. All accounts must be uniquely identifiable using the assigned username.
- iii. Shared accounts are not permitted.
- iv. All default passwords for accounts must be constructed in accordance with the CJIS Password Policy.
- v. All accounts must have a password expiration that complies with the CJIS Password Policy.
- vi. Concurrent connections may be limited for technical or security reasons.

- vii. All accounts must be disabled immediately upon notification of any employee's separation or termination.
- B. Account Management - The following items apply to system administrators or designated staff:
 - i. Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.
 - ii. All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
 - iii. Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.
 - iv. All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
 - v. Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third party account is found to be inactive for 30 days, the owners (of the account) and their manager will be notified of pending disablement. If the account continues to remain inactive for 15 days, it will be manually disabled.
 - vi. A list of accounts, for the systems they administer, must be provided when requested by authorized Myrtle Beach Police Department.
 - vii. An independent audit review may be performed to ensure the accounts are properly managed.
- C. Account Validation
 - i. All active directory user and NCIC user accounts shall be reviewed at least every six months. User accounts will be reviewed by the City of Myrtle Beach IT and/or their designee and NCIC user accounts will be reviewed by the terminal agency coordinator (TAC) or their 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.
 - ii. For all user accounts, the responsible party (City IT or 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.)

- iii. City IT and 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).
- iv. City IT and/or the TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.
- v. Primary responsibility for account management belongs to City IT and the Terminal Agency Coordinator (TAC). They are responsible for:
 - 1. Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
 - 2. Periodically review existing accounts for validity (at least once every 6 months), and
 - 3. Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.