
# Account Management Policy

12 Dec 2025

| | |
|---|---|
| **Authored By** | Reece Niemuth |
| **System Identifier** | PCOS-Homelab |
| **Date of Latest Revision** | 12 Dec 2025 |
| **Publication Version** | Revision 1 (1.0.0) |

CONTAINS NO CLASSIFIED OR SENSITIVE INFORMATION. THIS ARTIFACT SERVES TO DOCUMENT, IN PROFESSIONAL MANNER, A TRAINING RESOURCE FOR SELF-EDUCATION IN THE FIELD OF FEDERAL SYSTEMS ENGINEERING, MAINTENANCE, CYBERSECURITY RESEARCH, AND RELATED.

# Account Management Policy : Revision History

| Revision / Version | Date | Description / Notes |
|---|---|---|
| Rev. 1 (1.0.0) | 12 Dec 2025 | Publication Inception / Creation |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## 1. Purpose

The purpose of this Account Management Policy is to define the requirements and procedures for the creation, management, use, monitoring, and removal of user and system accounts within the Patriot Command Operations System (PCOS. This policy ensures that access to PCOS resources is controlled, auditable, and aligned with the principles of least privilege and separation of duties.

## 2. Scope

This policy applies to all accounts that access PCOS resources, including user accounts, privileged accounts, and service or system accounts. It applies to all PCOS components, whether physical or virtual, and encompasses operating systems, applications, network devices, security tools, and supporting infrastructure.

## 3. Account Types

PCOS supports the following account categories:

### 3.1 Standard User Accounts

Accounts assigned to individuals requiring non-privileged access to perform authorized functions.

### 3.2 Privileged Accounts

Accounts with elevated permissions used to perform administrative, configuration, or security functions. Privileged access is restricted to authorized personnel and used only when required.

### 3.3 Service and System Accounts

Non-interactive accounts used by applications, services, or automated processes. These accounts are configured with the minimum permissions required and are not used for interactive logon.

## 4. Account Lifecycle Management

### 4.1 Account Creation

Accounts are created only upon documented authorization and are assigned privileges consistent with approved roles. Default credentials are changed prior to use.

### 4.2 Account Modification

Account permissions are reviewed and updated when role changes occur. Unauthorized privilege escalation is prohibited.

### 4.3 Account Review

All accounts are reviewed at defined intervals to validate continued need, appropriate privilege levels, and compliance with system requirements.

### 4.4 Account Deactivation and Removal

Accounts are disabled or removed promptly when no longer required, including upon role change, inactivity, or termination of access.

## 5. Privileged Access Management

Privileged accounts are subject to additional controls, including:

- Separation between standard and privileged accounts
- Use of privileged access only for administrative functions
- Enhanced monitoring and logging of privileged activity
- Restrictions on shared or generic privileged accounts

## 6. Authentication and Credential Management

All accounts must use approved authentication mechanisms and credential policies. Passwords, keys, or certificates are protected from unauthorized disclosure. Credential reuse, sharing, or hardcoding is prohibited.

## 7. Monitoring and Auditing

Account activity is logged and monitored to detect unauthorized access, misuse, or anomalous behavior. Account-related events, including creation, modification, and deletion, are auditable and retained in accordance with established logging and monitoring procedures.

## 8. Inactive and Dormant Accounts

Accounts that remain inactive beyond defined thresholds are reviewed and disabled or removed to reduce risk. Service accounts are reviewed periodically to validate continued operational need.

## 9. Incident Handling

Suspected or confirmed account compromise, misuse, or unauthorized access must be reported immediately to the designated security authority (ISSO/ISSM). Account-related incidents are handled in accordance with established incident response procedures.

## 10. Enforcement

Failure to comply with this Account Management Policy may result in suspension or revocation of system access, corrective actions, or additional administrative measures as appropriate.

## PCOS References – Account Management Policy

1) **NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations**
   - *AC-2, AC-5, AC-6, IA-2, IA-5 Control Families*

2) **NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**
   - *Identification and Authentication*

3) **NIST SP 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems**
   - *Secure System Governance Principles*