Patriot Command Operations System (PCOS)

"Fortiter et Fideliter"

A living testbed for secure configuration, continuous monitoring, and automation — engineered to elevate my ability to protect information, sustain operations, and support the mission of the DoD cyber landscape

User Access Management Plan

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.

User Access Management Plan : Revision History

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

1. Purpose

The purpose of this User Access Management Plan is to define how **user accounts, privileges, and access rights** are managed within the **Patriot Command Operations System (PCOS)**.
This plan ensures that access to system resources is **authorized, controlled, documented, and appropriate to user roles**, while remaining practical for a **single-operator laboratory environment**.

2. Scope

This plan applies to all **logical access** to PCOS resources, including:

- Servers, workstations, and virtual machines
- Network and security management interfaces
- Administrative and monitoring platforms
- Supporting infrastructure and services

This plan governs:

- Account creation and removal
- Privilege assignment
- Access review practices
- Guest and temporary access

3. Access Control Principles

User access within PCOS is governed by the following principles:

- **Least Privilege** – Users are granted only the access required to perform their intended function
- **Role-Based Access** – Access is aligned to defined roles rather than individuals
- **Accountability** – All access is attributable to an identified user account
- **Separation of Activities** – Administrative access is limited and intentionally controlled

PCOS prioritizes **discipline and realism** over full-scale enterprise enforcement.

4. User Roles

4.1 System Owner / Administrator (Primary Role)

The PCOS System Owner serves as the **primary administrator** and is responsible for:

- System configuration and maintenance
- Security control implementation
- User account approval and management
- Monitoring and reviewing access activity

This role maintains **administrative privileges** across PCOS components.

4.2 Standard User (Optional / Limited)

Standard user accounts may exist for:

- Basic system interaction
- Non-privileged testing or review activities

These accounts:

- Do not have administrative rights
- Are restricted to specific systems or functions
- Are created only when necessary

4.3 Guest / Temporary Access

Guest or temporary access may be granted for:

- System review
- Functional testing
- Demonstrations
- Controlled cybersecurity exercises

Guest access is:

- Time-bound
- Limited in scope
- Disabled or removed after use

Guest accounts are **not intended for persistent system access**.

5. Pentesting and CTF Activities

Occasional **penetration testing or Capture-the-Flag (CTF)** activities may be conducted within PCOS by trusted participants.

Key considerations:

- Participants may be granted **temporary, restricted access**
- Activities are performed in **designated systems or segments**
- All pentesting and CTF activity is **documented separately** in the artifact titled: **“Penetration Testing Activities, Reports, and Remediation” (Located HERE)**

This User Access Management Plan governs **account authorization only**; technical testing scope, rules of engagement, findings, and remediation are addressed in the separate artifact.

6. Account Management

6.1 Account Creation

User accounts are created only when:

- There is a defined purpose
- Access is approved by the System Owner
- The access level is documented

Each account is uniquely identifiable and assigned to a single user.

6.2 Privilege Assignment

- Administrative privileges are restricted to the System Owner
- Elevated privileges are granted sparingly and only when required
- Guest and test accounts are **non-privileged by default**

6.3 Account Modification

Access changes may occur due to:

- Changes in testing scope
- Completion of a temporary activity
- Security or operational needs

All changes are documented informally through PCOS logs or notes.

6.4 Account Removal

Accounts are disabled or removed when:

- Access is no longer required
- Testing or review activities are complete
- An account is no longer actively used

7. Authentication Practices

PCOS uses standard authentication mechanisms appropriate to the platform, including:

- Local or directory-based authentication
- Strong passwords consistent with modern OS defaults
- Administrative authentication separation where supported

Multi-factor authentication (MFA) may be implemented where practical but is not mandatory for all components.

8. Access Review

Access reviews are conducted:

- Periodically, or
- When system changes occur

Given the limited number of users, reviews focus on:

- Verifying that only expected accounts exist
- Ensuring no unused or unnecessary accounts remain
- Confirming administrative access is appropriately restricted

9. Logging and Monitoring

Where supported by the platform:

- User authentication events are logged
- Administrative actions are auditable

- Logs may be centralized for review

Detailed analysis and alerting is handled through existing logging and monitoring capabilities.

10. Exceptions and Limitations

PCOS is a **non-regulated, single-operator laboratory environment**. As such:

- Access management practices are intentionally simplified
- Formal approval workflows and periodic audits are lightweight
- The focus is on **learning, realism, and disciplined operation**, not full enterprise enforcement

Any deviations from this plan are handled pragmatically and documented where appropriate.

11. Review and Maintenance

This plan is reviewed:

- At least annually, or
- When significant changes to user access occur

Updates are made as the system evolves.