
# Acceptable Use Policy (AUP)

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.

# Acceptable Use Policy (AUP) : Revision History

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

## 1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to define the authorized and acceptable use of the Patriot Command Operations System (PCOS) and its associated information systems, networks, hardware, software, and data. This policy establishes user responsibilities to protect the confidentiality, integrity, and availability of system resources and ensures compliance with applicable cybersecurity, operational, and governance requirements.

## 2. Scope

This policy applies to all individuals with authorized access to PCOS resources, including but not limited to system administrators, standard users, and service accounts. It applies to all PCOS components, whether physical or virtual, and includes servers, endpoints, network devices, storage systems, monitoring tools, and security platforms.

## 3. Authorized Use

Users are permitted to access and use PCOS resources solely for authorized purposes consistent with system objectives, approved roles, and assigned privileges. Authorized use includes:

- Performing approved administrative, operational, or security-related functions
- Conducting system monitoring, testing, configuration, and maintenance activities
- Supporting cybersecurity assessment, training, and research objectives aligned with PCOS
- Accessing data and services necessary to fulfill assigned responsibilities

All access must adhere to the principle of least privilege and follow established access control procedures.

## 4. Prohibited Use

The following activities are strictly prohibited on PCOS systems:

- Unauthorized access, modification, deletion, or disclosure of system data
- Installation or execution of unapproved software, scripts, or tools
- Circumventing security controls, monitoring mechanisms, or access restrictions
- Introducing malicious logic, unauthorized code, or unverified external media
- Using system resources for personal, commercial, or non-approved purposes

- Disabling or altering logging, auditing, or security monitoring capabilities

Any attempt to bypass system safeguards or exceed authorized privileges constitutes a policy violation.

## 5. Account and Credential Responsibilities

Users are responsible for safeguarding their authentication credentials and must not share accounts or passwords. Credentials must be used only by the individual or service for which they were issued. Users must immediately report suspected credential compromise, unauthorized access, or anomalous account activity.

## 6. Monitoring and Privacy

PCOS systems are subject to continuous monitoring, logging, and auditing to ensure security, operational integrity, and compliance. Users should have no expectation of privacy when using PCOS resources. System activity may be reviewed by authorized personnel for security, compliance, and investigative purposes.

## 7. Data Handling and Protection

Users must handle system data in accordance with approved data protection practices and security requirements. Data may not be copied, transferred, or stored outside of authorized PCOS locations without explicit approval. External storage devices and removable media are restricted and must comply with established media protection procedures.

## 8. Incident Reporting

Users must promptly report suspected security incidents, policy violations, system anomalies, or unsafe conditions to the designated security authority (ISSO/ISSM). Timely reporting supports effective incident response and risk mitigation.

## 9. Enforcement

Failure to comply with this Acceptable Use Policy may result in suspension or revocation of system access, corrective actions, or further administrative measures as appropriate. Violations may also trigger formal incident response and documentation processes.

## 10. Acknowledgment

By accessing or using PCOS systems, users acknowledge that they have read, understand, and agree to comply with this Acceptable Use Policy and all applicable system security requirements.

## PCOS References – Acceptable Use Policy

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

2) **NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**
   - *General User Responsibilities*

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