Whitelist of Approved Software

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.

Whitelist of Approved Software : Revision History

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

1. Purpose

The purpose of this document is to define the **Whitelist of Approved Software** authorized for installation and execution within the **Patriot Command Operations System (PCOS)** environment.
This whitelist supports system security, stability, and integrity by ensuring that only **approved, necessary, and trusted software** is permitted to operate on PCOS components.

This document implements disciplined configuration management practices consistent with federal information system security principles.

Click here to view the table of approved and applied software on the system.

2. Scope

This policy applies to **all PCOS system components**, including but not limited to:

- Domain Controllers
- Servers (e.g., logging, monitoring, vulnerability scanning)
- Administrative workstations
- Virtual machines
- Network and infrastructure management platforms

The whitelist applies to:

- Operating systems
- System services and agents
- Administrative and security tooling
- Supporting utilities required for system operation

3. Policy Statement

Only software explicitly listed on the **PCOS Approved Software Whitelist** is authorized for installation or execution within the PCOS environment.

Any software **not listed** is considered **unauthorized** and must not be installed or executed unless:

- It is formally reviewed, and
- It is approved through the PCOS configuration change process.

Unauthorized software may introduce security risks, reduce system integrity, or interfere with logging, monitoring, or authorization objectives.

4. Roles and Responsibilities

PCOS System Owner / ISSO

- Maintains and approves the Approved Software Whitelist
- Reviews and authorizes new software requests
- Ensures software aligns with system purpose and security objectives
- Periodically reviews the whitelist for accuracy and relevance

PCOS Operator (Single-Operator Environment)

- Installs and maintains only approved software
- Documents any software additions or removals
- Ensures software is sourced from trusted vendors or repositories

5. Software Approval Criteria

Software may be approved for inclusion on the whitelist if it meets the following criteria:

- Serves a **clear operational, security, or administrative purpose**
- Is sourced from a **trusted and reputable vendor or repository**
- Is compatible with the PCOS system architecture
- Does not introduce unnecessary services, telemetry, or attack surface
- Supports system logging, monitoring, or security posture where applicable

Preference is given to:

- Vendor-supported software
- Security-focused tools
- Widely adopted enterprise or federal-used platforms

6. Approved Software Categories

Approved software is categorized for clarity and control.

6.1 Operating Systems

- Server and workstation operating systems approved for PCOS use
- Includes core OS components, services, and default system utilities

6.2 Security and Monitoring Tools

- Logging, auditing, monitoring, and vulnerability assessment tools
- Agents and services required to support continuous monitoring objectives

6.3 Infrastructure and Administration Tools

- Directory services, DNS, identity management, and system administration utilities
- Hypervisor and virtualization management platforms

6.4 Network and Platform Management

- Firewall, switch, and network management interfaces
- Configuration and performance monitoring tools

6.5 Supporting Utilities

- Backup, synchronization, compression, and diagnostic utilities
- Utilities required to support secure operations and maintenance

7. Software Inventory Format

Each approved software entry should include, at minimum:

- Software Name
- Vendor / Source
- Version or Version Range
- System / Component Scope
- Purpose / Function
- Approval Status

The Approved Software Whitelist may be maintained as a controlled table (e.g., spreadsheet or document) referenced by this policy.

8. Software Changes and Exceptions

8.1 Additions

- New software must be evaluated prior to installation
- Approved additions are documented and added to the whitelist
- Significant additions should be recorded in the PCOS Maintenance or Change Log

8.2 Removals

- Software no longer required should be removed
- Whitelist entries should be updated accordingly

8.3 Temporary or Emergency Use

- Temporary use of non-listed software should be minimized
- Any temporary approval should be documented and time-bound

9. Review and Maintenance

The Approved Software Whitelist is a **living document** and will be reviewed:

- At least annually, or
- Following significant system changes

The review ensures the whitelist remains accurate, relevant, and aligned with PCOS operational objectives.

10. Compliance and Alignment

This document aligns with the intent of the following guidance:

- NIST SP 800-53 (Configuration Management and System Integrity principles)
- NIST SP 800-160 (Secure-by-Design and lifecycle engineering concepts)
- RMF-based authorization practices

PCOS is a non-regulated, single-operator environment; however, controls and processes are intentionally designed to **mirror enterprise and federal best practices** for realism, training, and discipline.

Current Approved and Applied Software Whitelist

Software Name	Vendor / Source	Approved Version	System Scope	Purpose / Justification
Windows Server 2022 Standard	Microsoft	Current Supported	COMMAND	Core server OS supporting AD DS and DNS
Active Directory Domain Services	Microsoft	Built-in Role	COMMAND	Centralized identity and authentication
DNS Server Role	Microsoft	Built-in Role	COMMAND	Name resolution for PCOS domain
RSAT / AD Admin Center	Microsoft	Current Supported	Reeces_PC	Secure directory administration
Splunk Universal Forwarder	Splunk	Current Stable	COMMAND	Audit and security log forwarding
Windows Defender AV	Microsoft	Built-in	COMMAND	Host-based malware protection
.NET Framework 4.x	Microsoft	Supported Versions	COMMAND	Application dependency
PowerShell 7	Microsoft	Current Stable	COMMAND	Secure administration and automation
Windows Server 2022	Microsoft	Alternate OS - 2022	COMMAND	Platform for monitoring and scanning tools
Splunk Enterprise	Splunk	500MB Free License	UNION	Centralized log aggregation and analysis
Splunk Universal Forwarder	Splunk	Current Stable	All Nodes (Except UNION)	Log collection and forwarding
Nessus Manager	Tenable	Current Stable	UNION	Centralized vulnerability scanning
Nessus Agent	Tenable	Current Stable	All Nodes (Except UNION)	Local vulnerability assessment
Python 3.x	Python Foundation	Supported Versions	Splunk Server	Required runtime for Splunk apps
OpenSSL, libcurl	Open Source	OS-supported	Servers	Secure communications
Git	Git SCM	Current Stable	Servers	Configuration and code management
PowerShell 7 / Bash	Microsoft / GNU	Current Stable	Servers	Administrative scripting
Ansible	Red Hat	Current Stable	Linux Nodes	Configuration management
Docker / Podman	Docker / Red Hat	Current Stable	Servers	Application isolation
Visual Studio Code	Microsoft	Current Stable	Admin Workstations	Secure scripting and config editing
Hyper-V	Microsoft	Built-in	Windows Hosts	Virtual machine hosting
Windows 11 Pro	Microsoft	Current Supported	Admin / Host Systems	Administrative workstation OS

Windows Server 2022	Microsoft	Current Supported	Hosts	Server workloads
Linux (Proxmox / Ubuntu / Rocky)	Open Source	LTS / Stable	Hypervisors	Virtualization and services
GRUB	GNU	OS Default	Linux Hosts	Secure boot management
Python 3	Python Foundation	Supported	All Systems	Automation and tooling
Git	Git SCM	Current Stable	All Systems	Configuration tracking
QEMU / KVM	Open Source	OS Default	Linux Hosts	VM virtualization
Docker / Podman	Docker / Red Hat	Current Stable	All Systems	Container support
Splunk Universal Forwarder	Splunk	Current Stable	All Systems	Log forwarding
TrueNAS / Synology DSM	iXsystems / Synology	Current Stable	LIBERTY	Centralized storage
SMB / NFS Services	Built-in	OS Default	LIBERTY	File sharing services
Built-in NAS Antivirus	Vendor Provided	If Available	LIBERTY	Malware protection
Node Exporter	Prometheus	Current Stable	LIBERTY	Performance monitoring
Snapshot & Replication Engine	Built-in	OS Default	LIBERTY	Backup and recovery
pfSense / OPNsense	Netgate / OPNsense	Current Stable	AREA51	Network boundary protection
pfBlockerNG / Threat Feeds	Open Source	Current Stable	AREA51	IP and DNS blocking
WireGuard / OpenVPN	Open Source	Current Stable	AREA51	Secure remote access
Telegraf / Node Exporter	InfluxData / Prometheus	Current Stable	AREA51	Metrics and telemetry
Windows 11 Pro	Microsoft	Current Supported	Reeces_PC	Administrative operations
Microsoft Office / O365	Microsoft	Current Subscription	Reeces_PC	Documentation and reporting
Visual Studio Code	Microsoft	Current Stable	Reeces_PC	Script and config editing
Vulnerator	Open Source	Current Stable	Reeces_PC	Vulnerability analysis
STIG Viewer	DISA	Current Release	Reeces_PC	STIG review
OpenSCAP / SCAP Workbench	Open Source	Current Stable	Reeces_PC	SCAP evaluation
Git	Git SCM	Current Stable	Reeces_PC	Source control
Python 3.x	Python Foundation	Supported	Reeces_PC	Automation
Ansible	Red Hat	Current Stable	Reeces_PC	Configuration automation
Nessus Agent	Tenable	Current Stable	Reeces_PC	Local scanning
Splunk Universal Forwarder	Splunk	Current Stable	Reeces_PC	Log forwarding
Docker Desktop	Docker	Current Stable	Reeces_PC	Local testing
Adobe Reader / Equivalent	Adobe	Current Stable	Reeces_PC	PDF review
Brave / Chrome	Brave / Google	Current Stable	Reeces_PC	Admin and research access
Raspberry Pi OS Lite	Raspberry Pi Foundation	Current Stable	DRONE	Lightweight monitoring host
Prometheus	CNCF	Current Stable	DRONE	Metrics collection

Node Exporter	Prometheus	Current Stable	DRONE	System metrics
Grafana	Grafana Labs	Current Stable	DRONE	Dashboard visualization
Python	Python Foundation	Supported	DRONE	Automation
systemd, OpenSSL, curl	OS Default	OS Default	DRONE	Core services
NIST OSCAL Tools	NIST	Current Stable	Engineering Systems	Machine-readable RMF artifacts
OpenSSL	Open Source	OS Supported	Engineering Systems	Secure communications
Wireshark	Wireshark Foundation	Current Stable	Reeces_PC	Packet inspection
CIS-CAT Lite	CIS	Current Stable	Reeces_PC	Benchmark assessment
GitHub CLI	GitHub	Current Stable	All Systems	Repo management
Python Requests / REST Libraries	Open Source	Current Stable	All Systems	API automation
Cloud-Init / Kickstart	Open Source	Current Stable	All Systems	Automated provisioning
Sysmon	Microsoft	Current Stable	Windows Systems	Security event logging

11. Approval

This Whitelist of Approved Software is approved by the PCOS System Owner and is effective upon publication.

Approved By:
Reece Niemuth
PCOS System Owner / ISSO

Effective Date:
12 Dec 2025