Security Categorization: Representative
(Modeled after System Controls with various Impact Levels)

Information System Contingency / Continuity of Operations Plan (ISCP / COOP)

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.

PCOS - ISCP / COOP : Revision History

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

1.1 PLAN APPROVAL

As the designated authority for the Patriot Command Operations System (PCOS), I hereby certify that this Information System Contingency Plan (ISCP / COOP) is complete and provides an accurate representation of the system, its architecture, and its recovery strategy. This plan reflects a best-effort implementation of NIST SP 800-34 contingency planning practices within a non-production, representative cybersecurity lab environment.

This ISCP / COOP will be reviewed and exercised on a periodic basis (at least annually or following significant system changes) and maintained under version control.

System Owner: Reece Niemuth
Title: System Owner and ISSE (Simulated)
Date: 12 Dec 2025

1. Introduction

The PCOS supports cybersecurity operations, testing, documentation development, and training activities. While non-production in nature, continuity of operations is necessary to maintain system availability for ongoing research, skill sustainment, and artifact development.

This ISCP / COOP establishes procedures to ensure continuity and timely recovery of PCOS following a disruptive event.

1.1 Background

This *PCOS* ISCP / COOP establishes procedures to recover *PCOS* following a disruption. The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Activation and Notification phase*** to activate the plan and determine the extent of damage;
  - ***Recovery phase*** to restore *PCOS* operations; and
  - ***Reconstitution phase*** to ensure that *PCOS* is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out PCOS processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *PCOS System Owner* personnel and provide guidance for recovering *PCOS* during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for *PCOS System Owner* contingency planning strategies. Ensure coordination with external points of contact and vendors associated with *PCOS* and execution of this plan.

1.2 Scope

This ISCP / COOP applies to the Patriot Command Operations System (PCOS), a standalone, non-production cybersecurity lab environment. The plan is modeled after **high-impact system contingency planning practices** but scoped to a single-operator environment.

This plan:

- Covers disruptions exceeding **72 hours**
- Focuses on system-level continuity, not enterprise business continuity
- Does not address short-duration outages or user-desktop data loss

1.3 Assumptions

The following assumptions were used when developing this ISCP / COOP:

- *PCOS is non-production and supports training, research, and documentation*
- *System owner is the sole operator and decision authority*
- *Backups are available locally and/or offline*
- *No geographically separate alternate site is maintained*
- *Recovery may require manual rebuild using documented baselines*

*This ISCP / COOP does **not** replace:*

- *Business Continuity Plans (BCP)*
- *Emergency evacuation procedures*
- *Physical safety response plans*

The *PCOS* ISCP / COOP does not apply to the following situations:

- **Overall recovery and continuity of mission/business operations.** The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) addresses employee evacuation.
- *Any additional constraints and associated plans should be added to this list.*

2. Concept of Operations

The Concept of Operations section provides details about *PCOS*, an overview of the three phases of the ISCP / COOP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of the PCOS personnel during a contingency activation.

See PCOS Official Concept of Operations (CONOPS) here.

2.1 System Description

PCOS consists of segmented infrastructure including:

- *pfSense firewall (AREA51)*
- *Managed switch (USLINK)*
- *Windows and Linux servers (COMMAND, UNION, STAR, EAGLE)*
- *NAS storage (LIBERTY)*
- *Monitoring node (DRONE)*

The system is hosted at a single residential location and supports simulated ISSO/ISSE operations.

2.2 Overview of Three Phases

This ISCP / COOP has been developed to recover the *PCOS* using a three-phased approach. This approach ensures that system recovery efforts are performed in a methodical sequence to maximize the effectiveness of the recovery effort and minimize system outage time due to errors and omissions.

The three system recovery phases are:

1) **Activation and Notification:** Triggered by extended outages, equipment failure, or environmental disruption. Initial assessment determines recovery feasibility.

2) **Recovery:** System components are restored in priority order using documented baselines and backups.

3) **Reconstitution:** Recovered systems are validated, tested, and returned to normal operation. Documentation and lessons learned are captured.

2.3 Overview of Three Phases

Role (*Single User Simulation*)	Responsibility
System Owner / ISCP Director	Authorizes activation and recovery
ISCP Coordinator	Coordinates recovery actions
Technical Recovery Lead	Executes rebuild and restoration
Documentation Authority	Updates plans and records lessons learned

The following persons or roles may activate the ISCP / COOP if one or more of these criteria are met:

Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.

3.2 Notification

Notification is performed by the system owner using:

- Direct system status review
- Manual documentation update
- Logged activation decision

3.3 Outage Assessment

Assessment includes:

- Root cause identification
- Hardware/software impact evaluation
- Estimated recovery timeline
- Resource availability review

4. Recovery

The Recovery Phase provides formal recovery operations that begin after the ISCP / COOP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, *PCOS* will be functional and capable of performing the functions identified in Section 2.1 of this plan.

4.1 Sequence of Recovery Activities

The following activities occur during recovery of *PCOS:*

1. Restore network boundary controls
2. Restore identity and authentication services
3. Restore security monitoring and scanning platforms
4. Restore storage and backups
5. Restore auxiliary services

4.2 Recovery Procedures

The following procedures are provided for recovery of *PCOS* at the original or established alternate location. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

Recovery of the PCOS is executed using:

- Hardware and software baselines
- Manual OS reinstallation if required
- Backup restoration from NAS or offline media

4.3 Recovery Escalation Notices/Awareness

Escalation is internal and documented in recovery logs. Status updates are recorded in system documentation.

5. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

5.1 Concurrent Processing

High-impact systems are not required to have concurrent processing as part of the validation effort. If concurrent processing does occur for the system prior to making it operational, procedures should be inserted here. Procedures should include length of time for concurrent processing, processing information on both concurrent systems, and validating information on the new permanent system.

For high-impact systems without concurrent processing, this section may either be removed or the following may be used:

In concurrent processing, a system operates at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly. *PCOS* does not have concurrent processing as part of validation. Once the system has been tested and validated, it will be placed into normal operations.

5.2 Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. The following procedures will be used to determine that the recovered data is complete and current to the last available backup:

- *Verify backup integrity*
- *Confirm configuration baselines*
- *Validate log continuity*

5.3 Validation Functionality Testing

Validation functionality testing is the process of verifying that *PCOS* functionality has been tested, and the system is ready to return to normal operations.

- *Authenticate users*
- *Run vulnerability scanning tools*
- *Verify logging and monitoring*

5.4 Recovery Declaration

Upon successfully completing testing and validation, the *System Owner* will formally declare recovery efforts complete, and that *PCOS* is in normal operations. *PCOS* business and technical POCs will be notified by documentation updates reflected in system status records on GitHub and directory artifact.

5.5 Notifications (users)

PCOS business and technical POCs will be notified by documentation updates reflected in system status records on GitHub and directory artifact.

5.6 Cleanup

Temporary recovery artifacts are removed. Baselines and documentation are updated.

5.7 Offsite Data Storage

The PCOS, in it's current capacity and operational scope, does not have or expect to use offsite data storage. To replace this, the NAS device (LIBERTY) can be used to offload data needed for system recovery and remediation.

5.8 Data Backup

A full backup is performed following recovery to the NAS device (LIBERTY).

5.9 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP / COOP. It is the responsibility of each ISCP / COOP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP / COOP Coordinator.

Event Documentation to include:

- *Recovery timeline*
- *Actions taken*
- *Lessons learned*
- *Plan updates*

5.10 Deactivation

Once all activities have been completed and documentation has been updated, the *System Owner* will formally deactivate the ISCP / COOP recovery and reconstitution effort. Notification of this declaration will be provided via standard documentation updates and GitHub repository adjustment.

5.11 Business Impact Analysis (BIA) Reference

Business Impact Analysis (BIA), which is retained as a separate artifact for organization purposes, should be referenced alongside the ISCP / COOP here. Historical record of system failures warranting invocation of the ISCP / COOP will associate with an updated copy of the BIA, in the archive location of all current and past records of system BIA, which is accessed here.

PCOS - ISCP / COOP APPENDICES

APPENDIX A PERSONNEL CONTACT LIST

Provide contact information for each person with a role or responsibility for activation or implementation of the ISCP / COOP, or coordination with the ISCP / COOP. For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.

PCOS ISCP / COOP Key Personnel		
Key Personnel		**Contact Information**
ISCP / COOP Director	Reece Niemuth	*PCOS GitHub Repository Issue Submission*

APPENDIX B VENDOR CONTACT LIST

Vendor	Product / Service	General Support Phone	General Support Email / Portal
AT&T	Internet Service Provider	800-288-2020	https://www.att.com/support
Microsoft	Windows Server / Windows OS	800-642-7676	https://support.microsoft.com
Red Hat (Rocky Linux)	Enterprise Linux Platform	N/A (Community Supported)	https://forums.rockylinux.org
Debian Linux	Linux OS Distribution	N/A (Community Supported)	https://www.debian.org/support
Protectli	Firewall Hardware (pfSense)	N/A (Ticket-based)	https://protectli.com/support
Netgear	Managed Network Switch	888-638-4327	https://www.netgear.com/support
Beelink	Mini PC / Compute Hardware	N/A (Email-based)	support@beelink.com
HP (Hewlett-Packard)	Enterprise / Desktop Hardware	800-474-6836	https://support.hp.com
CyberPower	UPS / Power Protection	877-297-6937	https://www.cyberpowersystems.com/support
pfSense (Netgate)	Firewall Software Platform	N/A (Community / Docs)	https://docs.netgate.com
Nessus (Tenable)	Vulnerability Scanning	855-267-7044	https://www.tenable.com/support
OpenSCAP	SCAP Compliance Tooling	N/A (Open Source)	https://www.open-scap.org

APPENDIX C DETAILED RECOVERY PROCEDURES

1. Restore network boundary device (pfSense) from configuration backup
2. Rebuild domain controller using documented baseline
3. Restore security tooling (SIEM, vulnerability scanner)
4. Validate identity, logging, and monitoring
5. Restore remaining virtual machines

If the system relies totally on another group or system for its recovery and reconstitution (such as a mainframe system), information provided should include contact information and locations of detailed recovery and reconstitution procedures for that supporting system.

APPENDIX D ALTERNATE PROCESSING PROCEDURES

Alternate processing consists of limited manual documentation activities performed offline. No alternate automated processing site is maintained.

APPENDIX E SYSTEM VALIDATION TEST PLAN

This appendix includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The system validation test plan may include the regression or functionality testing conducted prior to implementation of a system upgrade or change.

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

☐ *System boots successfully*
☐ *Firewall rules loaded and active*
☐ *Authentication services available*
☐ *SIEM receiving logs*
☐ *Vulnerability scanner operational*
☐ *Backups accessible*

APPENDIX F ALTERNATE STORAGE, SITE, AND TELECOMMUNICATIONS

This appendix provides information for alternate storage, alternate processing site, and alternate telecommunications for the system. Alternate storage, site, and telecommunications information is required for high-impact systems, per NIST SP 800-53 Rev. 3. Refer to NIST SP 800-53 Rev. 3, for details on control specifics. Information that should be provided for each area includes:

Alternate Storage:
- *Location: Onsite NAS (LIBERTY)*
- *Type: Owner-managed storage*
- *Access: Physical access controlled by system owner*

Alternate Processing Site:
- *None established.*
- *System recovery is performed at the primary location only.*

Alternate Telecommunications:
- *None established.*
- *Recovery dependent on restoration of primary ISP service.*

APPENDIX G DIAGRAMS (SYSTEM AND INPUT/OUTPUT)

System Architecture Diagrams (Physical, Network, and SCTM are available here..

APPENDIX H HARDWARE AND SOFTWARE INVENTORY

Hardware Inventory / Hardware Baseline is available for review here.

Software Inventory / Software Baseline is available for review here.

APPENDIX I INTERCONNECTIONS TABLE

PCOS does not directly interconnect with any other systems.

APPENDIX J TEST AND MAINTENANCE SCHEDULE

Review Frequency: Annual
Trigger Events: Major configuration changes, hardware replacement

Test Type: Tabletop + limited functional recovery
Full failover testing not applicable (single-site system)

Step	Date Due	Responsible Party	Date Scheduled	Date Held
Identify failover test facilitator.	N/A	ISCP / COOP Coordinator	N/A	N/A
Determine scope of failover test (include other systems?).	N/A	ISCP / COOP Coordinator, Test Facilitator	N/A	N/A
Develop failover test plan.	N/A	Test Facilitator	N/A	N/A
Invite participants.	N/A	Test Facilitator	N/A	N/A
Conduct functional test.	N/A	Test Facilitator, ISCP / COOP Coordinator	N/A	N/A
Finalize after action report and lessons learned.	N/A	ISCP / COOP Coordinator	N/A	N/A
Update ISCP / COOP based on lessons learned.	N/A	ISCP / COOP Coordinator	N/A	N/A
Approve and distribute updated version of ISCP / COOP.	N/A	ISCP / COOP Director, ISCP / COOP Coordinator	N/A	N/A

APPENDIX K ASSOCIATED PLANS AND PROCEDURES

- *System Security Plan (SSP)*
- *Business Impact Analysis (BIA)*
- *Disaster Recovery Procedures*
- *Incident Response Procedures*

Review the above documentation by browsing the GitHub Repository.

APPENDIX L BUSINESS IMPACT ANALYSIS

Business Impact Analysis (BIA) Documentation (Past and Current) available here.