System Backup, Continuity & Restoration Policy (DRP/BCP)

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.

System Backup, Continuity & Restoration 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 policy is to define the approach for system backup, continuity planning, and restoration of services for the Patriot Command Operations System (PCOS). This policy ensures that critical system configurations, data, and security-relevant artifacts are protected against loss and can be restored following system disruption, failure, or compromise, in a manner consistent with the intended use of PCOS as a research, training, and cybersecurity upskilling environment.

2. Scope

This policy applies to all PCOS components, including servers, virtual machines, endpoints, network devices, storage platforms, and supporting security tools. It covers system configuration data, security artifacts, documentation, and operational data necessary to reconstitute the environment following an adverse event.

3. System Classification and Continuity Objectives

PCOS is classified as a **non-production, non-mission-critical system** used for cybersecurity research, training, testing, and skills development. As such:

- Continuity objectives prioritize **data integrity and recoverability** over strict uptime requirements
- Restoration focuses on **system reconstitution** rather than uninterrupted service
- Recovery strategies are designed to be **cost-effective, repeatable, and realistic**

This classification informs recovery time objectives (RTOs) and recovery point objectives (RPOs) that are appropriate for the system's purpose.

4. Backup Strategy

4.1 Backup Scope

Backups include, at a minimum:

- Virtual machine images and snapshots
- System configuration files
- Security tooling configurations (e.g., logging, scanning, monitoring)
- Documentation and authorization artifacts

User-generated transient data and test artifacts may be excluded where appropriate.

4.2 Backup Frequency

Backups are performed on a **scheduled and event-driven basis**, including:

- Periodic baseline backups
- Backups prior to significant system changes
- Ad hoc backups following major configuration milestones

4.3 Backup Storage

Backups are stored in logically separate locations from primary system components. Storage solutions prioritize integrity, accessibility, and protection from accidental modification or loss.

5. Continuity Planning Approach

PCOS continuity planning is based on the ability to **rebuild and restore** system functionality rather than maintain high availability. Continuity measures include:

- Documentation of system architecture and configurations
- Preservation of installation media and baseline configurations
- Use of repeatable deployment processes where feasible
- Identification of critical components required for system reconstitution

This approach supports rapid recovery while remaining consistent with the system's educational and research objectives.

6. Restoration and Recovery Procedures

Restoration activities focus on:

- Rebuilding infrastructure from known-good baselines
- Restoring system configurations and security controls
- Revalidating security tooling and monitoring capabilities
- Confirming system integrity prior to resuming normal use

Restoration procedures are documented and refined as the system evolves.

7. Testing and Validation

Backup and restoration procedures are periodically tested to validate effectiveness and identify improvement opportunities. Testing may include:

- Restoration of selected virtual machines or configurations
- Verification of backup integrity
- Walkthroughs of recovery procedures

Testing frequency and depth are commensurate with system purpose and complexity.

8. Roles and Responsibilities

- **ISSO**: Oversees backup, continuity, and restoration planning and ensures alignment with security requirements
- **System Administrator**: Implements and maintains backup and restoration mechanisms
- **Users**: Protect system data and report incidents that may affect system availability or integrity

9. Incident Response Integration

Backup and restoration activities support incident response and recovery efforts. Following a security incident or system failure, restoration actions are coordinated with incident response procedures to ensure evidence preservation and risk mitigation.

10. Enforcement

Failure to adhere to this policy may result in system recovery delays, data loss, or increased risk exposure. Deviations from defined procedures must be documented and approved by the appropriate authority.

PCOS References – System Backup, Continuity, and Restoration Policy (DRP/BCP)

1) **NIST SP 800-34 Contingency Planning Guide for Federal Information Systems**
   - *Contingency Planning Guide*

2) **NIST SP 800-160 Vol. 2 Developing Cyber Resilient Systems: A Systems Security Engineering Approach**
   - *Cyber Resiliency Engineering*