PCOS

System Security Plan (SSP)

System Identifier: PCOS-Homelab

29 Nov 2025

Authored by: Reece Niemuth

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 IDENTIFICATION

1.1. System Name/Title: Patriot Command Operations System (PCOS)

1.1.1. System Categorization: Low Impact on Confidentiality

1.1.2. System Unique Identifier: PCOS-Homelab

1.2. Responsible Organization: PCOS– Home Lab - Reece Niemuth

Name:	Home Lab Located in Personal Residence
Address:	N/A
Phone:	N/A

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI**):**

Name:	Reece Niemuth
Title:	All Titles (Simulated)
Office Address:	N/A
Work Phone:	N/A
e-Mail Address:	N/A

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	Reece Niemuth
Title:	All Titles (Simulated)
Office Address:	N/A
Work Phone:	N/A
e-Mail Address:	N/A

1.2.1.2. System Security Officer:

Name:	Reece Niemuth
Title:	All Titles (Simulated)
Office Address:	N/A
Work Phone:	N/A
e-Mail Address:	N/A

1.3. General Description/Purpose of System: What is the function/purpose of the system? The PCOS Home Lab Enclave is treated as a *Low* confidentiality system for design and training purposes. The environment does not process production CUI, but it simulates CUI-like artifacts (e.g., SSPs, SARs, POA&Ms, test log data) and applies protections consistent with a low-impact environment. Integrity and availability are treated as at least *low to moderate* to support realistic RMF and Federal Information System Development and Maintenance.

1.3.1. Number of end users and privileged users: All privileged roles are currently held by the same individual (System Owner / ISSO) for purposes of the home lab. Separation of duties is simulated through distinct accounts and role definitions even when the same person fills multiple roles.

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users
1 (with various test user accounts)	1

1.4. General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

The PCOS Home Lab does not process real customer, corporate, or government CUI. Instead, it stores and processes CUI-like test data and artifacts to emulate a realistic environment

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

Github link to Overall System Architecture Documentation Repository: Click here

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Github link to Overall System Architecture Documentation Repository: Click here

2.2. List all software components installed on the system.

Github link to Overall System Architecture Documentation Repository: Click here

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization?

Yes, by myself, Reece Niemuth

3. REQUIREMENTS

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

NOTE: ALMOST ALL Requirements will be default to "Not Applicable" due to the lack of true CUI stored and processed by the PCOS Home Lab. This is an individual study and research approach to defense-related systems engineering and maintenance wherein the objective is not to support a federal customer or harbor any sensitive or classified information whatsoever.

3.1. Access Control

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI nor operational mission systems exist. Local AD and WireGuard access controls implemented only for lab environment segmentation.

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI access requirements. RBAC applied internally for learning purposes only.

3.1.3. Control the flow of CUI in accordance with approved authorizations.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI exists inside the simulated environment.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
Single-user test environment, no personnel roles. (unless simulated and documented)

3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

No privileges tied to CUI. Lab restricts admin access for practice only.

3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI; one primary user. Admin use controlled only for training scenarios.

3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
Single authorized user; no CUI-driven role enforcement.

3.1.8. Limit unsuccessful logon attempts.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
Security controls enabled only for lab simulation; not tied to CUI access.

3.1.9. Provide privacy and security notices consistent with applicable CUI rules.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
System not utilized by personnel or processing CUI.

3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable
Could configure Windows/Linux screen-lock timers for Zero Trust alignment.

3.1.11. Terminate (automatically) a user session after a defined condition.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI; idle session controls practiced as desired.

3.1.12. Monitor and control remote access sessions.

☒ Implemented ☐ Planned to be Implemented ☒ Not Applicable
WireGuard VPN with restricted network access; limited Zero Trust segmentation.

3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☒ Implemented ☐ Planned to be Implemented ☒ Not Applicable
WireGuard uses authenticated tunnels (ChaCha20-Poly1305) for secure access.

3.1.14. Route remote access via managed access control points.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
Remote access exists only for personal use; no CUI segregation required.

3.1.15. Authorize remote execution of privileged commands and remote access to security-relevant information.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
Single authorized individual; no privileged access to CUI.

3.1.16. Authorize wireless access prior to allowing such connections.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
Internal Wi-Fi does not support CUI; lab devices authorized locally.

3.1.17. Protect wireless access using authentication and encryption.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI handled. WPA3-Personal used only for general security posture.

3.1.18. Control connection of mobile devices.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No organizational mobile devices or CUI-bearing systems.

3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No CUI stored

3.1.20. Verify and control/limit connections to and use of external systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
External system connectivity not related to CUI flows.

3.1.21. Limit use of organizational portable storage devices on external systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No organizational portable media handling CUI.

3.1.22. Control CUI posted or processed on publicly accessible systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
No public exposure of CUI; lab is fully isolated to private home network.

3.2. Awareness and Training

3.2.1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A (no workforce)

3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A (self-learning only)

3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A (no insider threat to CUI)

3.3. Audit and Accountability

3.3.1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.3. Review and update logged events.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.4. Alert in the event of an audit logging process failure.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.6. Provide audit record reduction and report generation to support on-demand analysis and reporting.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.3.9. Limit management of audit logging functionality to a subset of privileged users.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Log retention and Splunk practice occurring only for simulation.

3.4. Configuration Management

3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.4. Analyze the security impact of changes prior to implementation.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.4.9. Control and monitor user-installed software.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Note:* SCAP/STIG configuration will be done for training purposes only.
(System Configurations are tracked via documentation updates and proper testing)

3.5. Identification and Authentication

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.5. Prevent reuse of identifiers for a defined period.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.6. Disable identifiers after a defined period of inactivity.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.8. Prohibit password reuse for a specified number of generations.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.10. Store and transmit only cryptographically-protected passwords.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.5.11. Obscure feedback of authentication information.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Lab MFA and password policy may be practiced but are not CUI-related.*

3.6. Incident Response

3.6.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *User may simulate and document IR tabletop exercises.*

3.6.2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *User may simulate and document IR tabletop exercises.*

3.6.3. Test the organizational incident response capability

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *User may simulate and document IR tabletop exercises.*

3.7. Maintenance

3.7.1. Perform maintenance on organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Self-maintained devices only. (Maintenance documented separately when / if needed)*

3.7.2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

N/A - *Self-maintained devices only. (Maintenance documented separately when / if needed)*

3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Self-maintained devices only. (Maintenance documented separately when / if needed)*

3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Self-maintained devices only. (Maintenance documented separately when / if needed)*

3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Self-maintained devices only. (Maintenance documented separately when / if needed)*

3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - *Self-maintained devices only. (Maintenance documented separately when / if needed)*

3.8. Media Protection

3.8.1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.2. Limit access to CUI on system media to authorized users.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.4. Mark media with necessary CUI markings and distribution limitations.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

N/A - No CUI on digital or physical media.

3.8.5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.7. Control the use of removable media on system components.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.8.9. Protect the confidentiality of backup CUI at storage locations.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI on digital or physical media.

3.9. Personnel Security

3.9.1. Screen individuals prior to authorizing access to organizational systems containing CUI.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Only one authorized user exists; no HR actions relevant to CUI.

3.9.2. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - Only one authorized user exists; no HR actions relevant to CUI.

3.10. Physical Protection

3.10.1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No authorized personnel roles, no CUI protection zones.

3.10.2. Protect and monitor the physical facility and support infrastructure for organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No authorized personnel roles, no CUI protection zones.

3.10.3. Escort visitors and monitor visitor activity.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No authorized personnel roles, no CUI protection zones.

3.10.4. Maintain audit logs of physical access.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No authorized personnel roles, no CUI protection zones.

3.10.5. Control and manage physical access devices.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No authorized personnel roles, no CUI protection zones.

3.10.6. Enforce safeguarding measures for CUI at alternate work sites.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No authorized personnel roles, no CUI protection zones.

3.11. Risk Assessment

3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No mission/business risk to CUI-bearing systems. (Informal Assessments are conducted)

3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No mission/business risk to CUI-bearing systems. (Informal Assessments are conducted)

3.11.3. Remediate vulnerabilities in accordance with risk assessments.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No mission/business risk to CUI-bearing systems. (Informal Assessments are conducted)

3.12. Security Assessment

3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No formal DoD authorization boundary. (General Testing will take place however)

3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No formal DoD authorization boundary. (General Testing will take place however)

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No formal DoD authorization boundary. (General Testing will take place however)

3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No formal DoD authorization boundary. (General Testing will take place however).

3.13. System and Communications Protection

3.13.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.3. Separate user functionality from system management functionality.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.13. Control and monitor the use of mobile code.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.15. Protect the authenticity of communications sessions.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.13.16. Protect the confidentiality of CUI at rest.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI transmitted or stored. (General Communication Security Practiced/Tested)

3.14. System and Information Integrity

3.14.1. Identify, report, and correct system flaws in a timely manner.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

3.14.2. Provide protection from malicious code at designated locations within organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

3.14.3. Monitor system security alerts and advisories and take action in response.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

3.14.4. Update malicious code protection mechanisms when new releases are available.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

3.14.5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

3.14.6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

3.14.7. Identify unauthorized use of organizational systems.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable
N/A - No CUI integrity requirements. (Integrity will be handled in general maintenance)

4. RECORD OF CHANGES

Date	Description	Made By:
29 Nov 2025	Initial PCOS SSP Artifact – Inception of SSP	Reece Niemuth