# 🔐 Cybersecurity Policy Index

The Contract Coach

CyberHygiene Production Network (CPN)

*Last Updated: November 2, 2025*

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

## 📋 Policy Documentation Package

This comprehensive policy package supports NIST SP 800-171 Rev 2 compliance and CMMC Level 2 certification. All policies have been customized for The Contract Coach's solopreneur business model and CyberHygiene Production Network environment.

**Owner/ISSO:** Donald E. Shannon | **Domain:** cyberinabox.net | **System Classification:** CUI (Controlled Unclassified Information)

*Note: Owner/ISSO holds active Top Secret (TS) personnel security clearance, exceeding CUI access screening requirements per 32 CFR Part 2002. System processes CUI only.*

| **7** | **11** | **50+** |
|:---:|:---:|:---:|
| Core Policy Documents | NIST Control Families | Individual Controls |

## +100

Est. SPRS Points

## 🚀 Quick Start - Begin Here

New to these policies? Start with the Policy Review and Approval Checklist. This comprehensive guide walks you through reviewing, approving, and implementing all policies in a systematic 4-6 hour process.

📖 **Open Implementation Checklist**

# 📚 Core Policy Documents

Click on any policy to open the full document. Each policy includes detailed procedures, command examples, and compliance mapping.

**TCC-IRP-001**

## Incident Response Policy and Procedures

Comprehensive incident detection, response, containment, eradication, and recovery procedures. Includes integration with Wazuh SIEM, FreeIPA, and Suricata IDS. Covers DoD 72-hour reporting requirements.

**NIST Families:**

**IR-1**   **IR-2**   **IR-3**   **IR-4**   **IR-5**   **IR-6**   **IR-7**

**IR-8**

📄 19KB      ⏱ ~25 min read      ✅ Complete

📖 **Open Policy**

**TCC-RA-001**

## Risk Management Policy and Procedures

Complete risk assessment framework with vulnerability management, supply chain risk assessment, and continuous monitoring. Includes Wazuh and OpenSCAP integration with defined remediation timelines.

**NIST Families:**

**RA-1**   **RA-2**   **RA-3**   **RA-5**   **RA-6**   **RA-7**

**RA-8**   **RA-9**

📄 25KB      ⏱ ~25 min read      ✅ Complete

📖 **Open Policy**

**TCC-PS-001**

## Personnel Security Policy

Personnel lifecycle management from onboarding to termination. Includes contractor vetting procedures, FreeIPA account provisioning, quarterly access reviews, and personnel security clearance documentation (Owner holds TS clearance exceeding CUI requirements).

**NIST Families:**

**PS-1**   **PS-2**   **PS-3**   **PS-4**   **PS-5**   **PS-6**

**PS-7**   **PS-8**

📄 24KB      ⏱️ ~25 min read      ✅ Complete

📖 **Open Policy**

**TCC-PE-MP-001**

## Physical and Media Protection Policy

Combined PE and MP families coverage. Home office physical security, locking server rack, LUKS encryption for all CUI media, media sanitization procedures, and environmental controls (UPS, HVAC, fire).

**NIST Families:**

**PE-1 to PE-20**   **MP-1 to MP-8**

📄 22KB      ⏱️ ~25 min read      ✅ Complete

📖 **Open Policy**

**TCC-SI-001**

## System and Information Integrity Policy

Flaw remediation with automated patching, malware protection (ClamAV), continuous monitoring (Wazuh SIEM), file integrity monitoring, security functionality verification with OpenSCAP, and vulnerability management.

**NIST Families:**

SI-1    SI-2    SI-3    SI-4    SI-5    SI-6    SI-7
SI-10 to SI-12

📄 21KB     ⏱ ~25 min read     ✅ Complete

📖 **Open Policy**

**TCC-AUP-001**

## Acceptable Use Policy

Comprehensive user responsibilities, prohibited activities, CUI marking requirements, password policy integration with FreeIPA, incident reporting procedures, and user acknowledgment form template.

**NIST Families:**

AC-1    PS-6    PL-4

📄 21KB     ⏱ ~20 min read     ✅ Complete

📖 **Open Policy**

SUMMARY

## Policy Documentation Summary

Executive overview of all policies, SPRS score impact assessment, CMMC readiness guidance, implementation roadmap, and recommendations for additional policies. Essential starting point for understanding the complete package.

**Purpose:**

**Overview**    **Implementation Guide**

**Compliance Assessment**

📄 22KB    ⏱️ ~30 min read    ✅ Complete

📖 **Open Summary**

## 📋 System Security Plan (SSP)

The authoritative security documentation for the CyberHygiene Production Network.

**SSP v1.4**     ✅ **CURRENT**

## System Security Plan (Version 1.4)

Complete unified SSP document with full system architecture, technical implementation details, all 14 control family implementations, integrated policy framework, unified POA&M (28 items), network diagrams, and system configuration. Includes all Version 1.4 policy integrations (IR, RA, PS, PE, MP, SI, AUP) with 98% implementation status.

**Contains:**

**System Architecture**     **14 Control Families**

**Policy Framework**     **Unified POA&M**

**Network Diagrams**     **Authorization**

📄 39KB     📅 Version 1.4: November 2, 2025     ✅ 98% Implementation

📖 **Open SSP v1.4**

---

**POA&M v1.4**     ✅ **CURRENT**

## Plan of Action & Milestones

Comprehensive tracking of all security weaknesses and remediation plans. Includes 28 items organized into 5 sections: Completed (16), In Progress (2), On Track (8), Planned (2), and New (7). Integrated as Section 10 of SSP v1.4.

**Status:**

**57% Complete**     **28 Total Items**

**8 High Priority**

📄 14KB     📅 Updated: November 2, 2025     📊 57% Complete (16/28)

📖 **Open POA&M**

---

📌 **SSP Version 1.4 Highlights:**

- **Unified Document:** Single comprehensive SSP with all policies integrated
- **Policy Framework:** All 7 core policies (IR, RA, PS, PE, MP, SI, AUP) fully referenced

- **POA&M Tracking:** 28 items with 57% completion rate
- **Implementation Status:** 98% complete, ready for authorization
- **SPRS Impact:** Estimated +90 to +110 points from policy implementation

**Version History:** v1.0 (Oct 26) → v1.1 (Oct 28) → v1.2 (Oct 31) → v1.3 (Oct 31) → **v1.4 (Nov 2, 2025 - Current)**

## 📚 Supporting Documents

Additional compliance and operational documentation.

## Implementation & Compliance

📄 Policy Review and Approval Checklist - Step-by-step implementation guide (4-6 hours)

📄 SPRS Update Guide - ⭐ NEW: Detailed SPRS assessment update instructions with control mapping

📄 Evidence Package Summary - ⭐ NEW: Complete CMMC Level 2 evidence package

📄 Control-to-Policy Quick Reference - ⭐ NEW: All 110 controls mapped to policies

📄 Backup Procedures - Daily and weekly backup procedures with ReaR

📄 Configuration Management Baseline - System baseline and change control

📄 Incident Response Plan - Detailed IR planning document

## Checklists & Controls

📄 Physical Security Controls - Physical protection measures

📄 Quarterly SSP Review Checklist - SSP maintenance tasks

📄 Samba FIPS Testing Checklist - FIPS compliance verification

## 🎯 Quick Access by Compliance Need

## 🚨 Incident Response

**Need to respond to a security incident?**

📄 Incident Response Policy - Complete procedures

📄 Incident Response Plan - Planning document

⏰ **Report CUI incidents to DoD within 72 hours**

## 👤 Onboarding Contractors

**Need to grant access to a contractor?**

📄 Personnel Security Policy - See Procedure 1: Contractor Onboarding

📄 Acceptable Use Policy - Provide to contractor, obtain signed acknowledgment

## 🔍 CMMC Assessment Prep

**Preparing for CMMC assessment?**

📄 Policy Documentation Summary - Assessment readiness checklist

📄 All 6 core policies - Evidence of institutionalized practices

📄 Quarterly SSP Review - Maintenance evidence

## 📊 SPRS Score Update

**Updating your SPRS score?**

📄 SPRS Update Guide - Detailed instructions with control-to-policy mapping

📄 Policy Documentation Summary - See SPRS Score Impact section

📄 Evidence Package Summary - Complete CMMC Level 2 evidence

📄 Use policies as evidence to change status from "Planned" to "Implemented"

📈 **Estimated impact: +90 to +110 points**

## 📋 System Security Plan

**Need your complete SSP documentation?**

📄 System Security Plan v1.4 - Complete unified SSP

📄 Unified POA&M - 28 items tracked (57% complete)

📄 All 7 core policies integrated (IR, RA, PS, PE, MP, SI, AUP)

📄 98% complete implementation with authorization recommendation

📅 **Version 1.4: November 2, 2025 (Current)**

# 📋 Policy Review Schedule

## Upcoming Reviews and Activities

📄 **Quarterly (Jan, Apr, Jul, Oct):**

    📄 Access review (Personnel Security Policy)

    📄 OpenSCAP compliance scan (Risk Management Policy)

    📄 Wazuh dashboard review (System Integrity Policy)

📄 Facility security inspection (Physical Security Policy)

📄 **Annual (November 2026):**

📄 Review and update all 7 policy documents

📄 Conduct risk assessment (Q1 2026)

📄 Conduct IR tabletop exercise (Q2 2026)

# 🔐 Security & Classification

### Document Handling Requirements

**Classification:** Controlled Unclassified Information (CUI)
**Storage Location:** `/backup/personnel-security/policies/` (encrypted partition)
**Access Control:** ISSO access only (file permissions 600)
**Backup:** Included in daily backup procedures
**Retention:** Retain for 3 years minimum (CMMC evidence)
**Distribution:** Owner/Principal + authorized contractors (with signed acknowledgment)

**ISSO/Owner:** Donald E. Shannon     **Email:** Don@contractcoach.com
**Phone:** 505.259.8485

The Contract Coach - CyberHygiene Production Network
Policy Index Last Updated: November 2, 2025

NIST SP 800-171 Rev 2 | CMMC Level 2 | FIPS 140-2