

Cybersecurity Protocol For Industrial Control Systems (ICS) Checklist 2026

Network Segmentation & Perimeter Defense

Verification of firewall configurations, DMZ implementation, and separation between IT and OT (Operational Technology) networks.

Network Perimeter Status

- ☐ Fully Segmented (IT/OT Air-Gapped/Firewalled)
- ☐ Partially Segmented
- ☐ No Segmentation Detected

Implemented Security Controls

- ☐ Firewall Implementation
- ☐ DMZ (Demilitarized Zone) Configuration
- ☐ Intrusion Prevention System (IPS)
- ☐ VLAN Implementation
- ☐ Unidirectional Gateways (Data Diodes)

Firewall Configuration Details

Write something...

Network Topology Diagram

 Upload File

Last Network Perimeter Audit Date

Enter date...

Network Security Engineer Verification

Access Control & Identity Management

Audit of user authentication protocols, multi-factor authentication (MFA) deployment, and Least Privilege Access (LPA) enforcement for all ICS operators.

MFA Deployment Status

- ☐ Fully Implemented
- ☐ Partially Implemented
- ☐ Not Implemented

Authenticated User Roles Verified

- ☐ Administrator
- ☐ Operator
- ☐ Engineer
- ☐ Viewer/Read-Only
- ☐ External Vendor

Last Access Review Date

Write something...

Identified Access Discrepancies or Vulnerabilities

Write something...

User Access Permission Matrix

 Upload File

Security Auditor Verification

Endpoint Protection & Device Security

Assessment of antivirus/anti-malware deployment on Human Machine Interfaces (HMIs), engineering workstations, and PLC protection measures.

HMI (Human Machine Interface) Antivirus Status

- ☐ Fully Updated
- ☐ Out of Date
- ☐ Not Installed
- ☐ Not Applicable

Protected Endpoints Identified

- ☐ Engineering Workstations
- ☐ HMIs (Human Machine Interfaces)
- ☐ Historian Servers
- ☐ Operator Terminals
- ☐ SCADA Servers

Last Security Scan Timestamp

Write something...

Antivirus Definition Report

 Upload File

Unresolved Security Vulnerabilities

Write something...

Security Officer Verification

Patch Management & Vulnerability Assessment

Review of firmware update schedules, critical vulnerability scanning, and testing protocols for security patches in production environments.

Last Vulnerability Scan Date

Enter date...

Critical Vulnerability Status

- ☐ No critical vulnerabilities identified
- ☐ Critical vulnerabilities identified - Remediation in progress
- ☐ Critical vulnerabilities identified - Urgent action required

Summary of Identified Vulnerabilities and Risk Assessment

Write something...

Patched Asset Categories

- ☐ PLC (Programmable Logic Controllers)
- ☐ HMI (Human Machine Interfaces)
- ☐ Engineering Workstations
- ☐ Network Switches/Routers
- ☐ Sensors & Actuators

Upload Scan Report/Patch Log

 Upload File

Security Officer Approval

Incident Response & Disaster Recovery

Evaluation of ICS-specific incident response plans, backup integrity for PLC logic, and system restoration procedures after a cyber event.

Last Incident Response Drill Date

Enter date...

Incident Severity Level

- ☐ Low (Minimal Operational Impact)
- ☐ Medium (Partial System Disruption)
- ☐ High (Critical Process Downtime)
- ☐ Critical (Total System Compromise/Safety Risk)

Recovered Systems Checklist

- ☐ PLC Logic & Firmware
- ☐ HMI Configuration Files
- ☐ SCADA Databases
- ☐ Network Switch Configurations
- ☐ Historian Data Archives

Incident Summary & Root Cause Analysis

Write something...

Upload Backup Verification Log

 Upload File

Incident Response Lead Authorization

Physical Security & Hardware Integrity

Inspection of physical access to control cabinets, USB port lockdowns, and monitoring of unauthorized hardware connections.

Control Cabinet Access Status

- ☐ Locked and Secured
- ☐ Unlocked/Tampered
- ☐ N/A

Physical Security Measures Present

- ☐ CCTV Surveillance
- ☐ Biometric Access Control
- ☐ Security Seals/Tamper-evident Tape
- ☐ Motion Sensors
- ☐ Security Badge Readers

Unused USB/Peripherals Check

Write something...

Identified Vulnerabilities or Physical Breaches

Write something...

Last Physical Inspection Date

Enter date...

Inspector Authorization

Monitoring, Logging & Threat Detection

Validation of continuous network monitoring, anomaly detection systems (IDS), and centralized logging of industrial protocol traffic.

IDS (Intrusion Detection System) Status

- ☐ Active & Monitoring
- ☐ Alerts Only
- ☐ Inactive/Not Implemented

Monitored Protocol Types

- ☐ Modbus
- ☐ PROFINET
- ☐ EtherNet/IP
- ☐ DNP3
- ☐ OPC UA

Last Security Log Review Date

Number of Unresolved Security Alerts

Enter a number...

Detected Anomalies & Observations

Write something...

Log Export/Audit Report Attachment



Upload File

Supply Chain & Third-Party Access Security

Verification of vendor remote access protocols, secure file transfer methods, and security compliance for hardware/software suppliers.

Vendor Access Level

- ☐ Full Remote Access
- ☐ Restricted/VPN Only
- ☐ On-site Only
- ☐ No Direct Access

Security Documentation Verified

- ☐ SOC2 Report
- ☐ ISO 27001 Certification
- ☐ Non-Disclosure Agreement (NDA)
- ☐ Cybersecurity Compliance Certificate

Last Security Audit Date of Vendor

Enter date...

Upload Vendor Security Assessment Form

 Upload File

Vendor Name and Contact Information

Write something...

Description of Risk Mitigation Measures for Third-Party Access

Write something...

Compliance Officer Approval

Employee Training & Security Awareness

Assessment of staff training programs regarding social engineering, phishing, and operational security hygiene for floor personnel.

Last Training Completion Date

Enter date...

Training Modules Completed

- ☐ Phishing Awareness
- ☐ Industrial Cybersecurity Fundamentals
- ☐ Secure Remote Access Protocols
- ☐ Incident Reporting Procedures
- ☐ Physical Security & Device Handling

Percentage of Staff Trained (Target vs. Actual)

Enter a number...

Training Gaps and Identified Weaknesses

Write something...

Training Attendance Logs & Certifications

 Upload File

Safety & Security Officer Verification

Audit Compliance & Continuous Improvement

Review of periodic security audits, documentation of security incidents, and alignment with international standards like IEC 62443.

Audit Completion Date

Compliance Standard Alignment

- ☐ IEC 62443
- ☐ NIST SP 800-82
- ☐ ISO/IEC 27001
- ☐ Internal Policy Only

Identified Non-Compliance Areas

- ☐ Network Configuration
- ☐ Access Management
- ☐ Patching Protocols
- ☐ Physical Security
- ☐ Employee Training

Corrective Action Plan (CAP) Details

Supporting Audit Documentation

 **Upload File**

Lead Auditor Signature

< Previous

> Next

✔ Finish

✎ Generate Sample Report