Industrial Automation Control Systems Security Policy

Document ID: POL-ICS-2024-001

Version: 3.2

Effective Date: January 15, 2024

Last Updated: January 11, 2024

Document Owner: Chief Security Architect

Classification: CONFIDENTIAL

1. Purpose and Scope

1. This Industrial Automation Control Systems (IACS) Security Policy establishes the security requirements and controls for the protection of industrial automation and control systems operated by DeepShield Systems, Inc. ("Company") and its clients.

2. This Policy applies to all operational technology (OT) environments, including but not limited to:

- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA) systems
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLCs)
- Human-Machine Interfaces (HMIs)
- Industrial IoT devices and sensors

2. Definitions

1. "Critical Infrastructure" refers to systems and assets, whether physical or virtual, so vital that their incapacity or destruction would have a debilitating impact on security, economic security, or public health or safety.

2. "Defense-in-Depth" means a layered security approach incorporating multiple defensive mechanisms to protect industrial control systems and networks.

3. "Security Zone" refers to a grouping of logical or physical assets that share common security requirements.

3. Security Architecture Requirements

1. Network Segmentation

- Implementation of ISA-99/IEC 62443 security zones and conduits
- Physical and logical separation between IT and OT networks
- Deployment of industrial demilitarized zones (iDMZ)
- Implementation of unidirectional security gateways where appropriate

2. Access Control

- Role-based access control (RBAC) for all IACS components
- Multi-factor authentication for administrative access
- Privileged Access Management (PAM) system implementation
- Regular access rights review and certification

3. Communication Security

- Encryption of all non-real-time control traffic
- Secure protocols for remote access (e.g., IPSec VPN)
- Protocol-specific security controls for industrial protocols
- Network traffic monitoring and analysis

4. Operational Security Controls

1. Change Management

- Documented change control procedures for all IACS modifications
- Security impact analysis for system changes
- Testing requirements for security patches and updates
- Roll-back procedures for failed changes

2. Incident Response

- Dedicated OT incident response team and procedures
- Integration with enterprise security operations center
- Regular testing of incident response procedures
- Mandatory incident reporting and escalation protocols

3. Backup and Recovery

- Regular backup of critical IACS configurations

- Secure offline storage of backup media
- Annual recovery testing requirements
- Documentation of system restoration procedures

5. Compliance and Audit

1. Standards Compliance
- Adherence to IEC 62443 series standards
- Compliance with NIST SP 800-82 guidelines
- Implementation of relevant ISA/IEC 62443 security levels
- Regular compliance assessments and reporting

2. Audit Requirements
- Annual security audits of IACS environments
- Quarterly vulnerability assessments
- Continuous security monitoring and logging
- Independent third-party security assessments

6. Training and Awareness

1. All personnel with access to IACS environments must complete:
- Initial OT security awareness training
- Annual security refresher training
- Role-specific technical security training
- Incident response and recovery procedures training

7. Policy Enforcement

1. Violations of this Policy may result in:
- Immediate revocation of system access
- Disciplinary action up to and including termination
- Legal action where applicable
- Reporting to relevant regulatory authorities

8. Policy Review and Updates

1. This Policy shall be reviewed and updated:

- Annually at minimum
- Following significant security incidents
- Upon major system architecture changes
- As required by regulatory changes

9. Approval and Authorization

This Policy is approved and authorized by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Date: January 11, 2024

10. Document Control

Version History:

- 3.2: January 2024 - Updated compliance requirements
- 3.1: July 2023 - Enhanced incident response procedures
- 3.0: January 2023 - Major revision incorporating IEC 62443 updates
- 2.1: July 2022 - Minor updates to access control requirements