# Industrial Control Systems Security Baseline

**DeepShield Systems, Inc.**

*Effective Date: January 15, 2024*

*Document Version: 2.4*

*Classification: Confidential*

## 1. Purpose and Scope

1. This Industrial Control Systems (ICS) Security Baseline ("Baseline") establishes the minimum security requirements and controls for all operational technology (OT) environments, industrial control systems, and related infrastructure operated by or on behalf of DeepShield Systems, Inc. ("Company").

2. This Baseline applies to all Company employees, contractors, consultants, temporary workers, and other business partners who interact with or manage industrial control systems.

## 2. Definitions

1. "Industrial Control System" or "ICS" means the combination of control components that act together to achieve an industrial objective, including SCADA systems, distributed control systems (DCS), programmable logic controllers (PLCs), remote terminal units (RTUs), and intelligent electronic devices (IEDs).

2. "Security Zone" refers to a grouping of logical or physical assets that share common security requirements based on criticality and sensitivity.

3. "Deep-Layer Architecture" means the Company's proprietary multi-layered security framework incorporating AI-driven threat detection and response capabilities.

## 3. Security Architecture Requirements

1. Network Segmentation

a) All ICS networks must implement a minimum of five security zones with defined trust boundaries

b) Implementation of air-gapped networks for critical control systems

c) Strict control of all communication paths between zones using managed interfaces

2. Access Control

a) Implementation of role-based access control (RBAC) for all ICS components

b) Multi-factor authentication for all privileged access

c) Unique credentials for each user and service account

d) Regular access rights review and certification

3. System Hardening

a) Removal of unnecessary services, applications, and protocols

b) Implementation of secure configurations based on Company-approved templates

c) Regular vulnerability assessments and security patches

d) Encryption of all sensitive data at rest and in transit

## 4. Monitoring and Incident Response

1. Continuous Monitoring

a) Real-time monitoring of all ICS network traffic

b) Implementation of Company's AI-driven anomaly detection system

c) Regular security metrics collection and analysis

d) Automated asset inventory and change detection

2. Incident Response

a) Maintenance of current incident response procedures

b) Regular testing of recovery and continuity plans

c) Integration with Company's Security Operations Center

d) 24/7 availability of incident response team

## 5. Compliance and Audit

1. All ICS environments must maintain compliance with:

a) NIST SP 800-82 Guidelines

b) IEC 62443 Standards

c) Company's proprietary security frameworks

d) Applicable regulatory requirements

2. Audit Requirements

a) Annual third-party security assessments

b) Quarterly internal security reviews

c) Continuous compliance monitoring

d) Regular penetration testing

## 6. Training and Awareness

1. Required Training

a) Annual ICS security awareness training for all personnel

b) Specialized training for ICS operators and administrators

c) Incident response and recovery procedures training

d) Regular security update briefings

## 7. Documentation and Change Management

1. Required Documentation

a) Current network architecture diagrams

b) System security plans

c) Standard operating procedures

d) Incident response playbooks

2. Change Management

a) Formal change control procedures

b) Security impact analysis requirements

c) Testing and validation protocols

d) Rollback procedures

## 8. Enforcement and Exceptions

1. Compliance with this Baseline is mandatory for all covered systems and personnel.

2. Exceptions must be:

a) Documented and risk-assessed

b) Approved by the Chief Security Architect

c) Reviewed quarterly

d) Time-limited with specific expiration dates

## 9. Review and Updates

1. This Baseline shall be reviewed and updated annually or upon significant changes to:

a) Technology infrastructure

b) Threat landscape

c) Regulatory requirements

d) Company security objectives

## Approval and Authorization

APPROVED AND ADOPTED by DeepShield Systems, Inc.

**By:**

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

**By:**

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024