Industrial Control System Security Guidelines

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: Confidential - Internal Use Only

1. Purpose and Scope

1. These Industrial Control System (ICS) Security Guidelines ("Guidelines") establish the minimum security requirements and operational procedures for the protection of industrial control systems, operational technology (OT) environments, and related critical infrastructure components managed or secured by DeepShield Systems, Inc. ("Company").

2. These Guidelines apply to all Company employees, contractors, consultants, temporary workers, and other personnel who interact with or support industrial control systems, including but not limited to SCADA networks, distributed control systems (DCS), programmable logic controllers (PLCs), and related OT infrastructure.

2. Definitions

1. "Industrial Control System (ICS)" refers to any combination of control components that act together to achieve industrial objectives, including manufacturing, transportation, energy distribution, or other critical infrastructure processes.

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

3. "Deep-Layer Security Architecture" refers to the Company's proprietary multi-layered security framework for protecting industrial control systems.

3. System Access Control

1. Access Management

a) All access to ICS environments shall be granted on a least-privilege basis

b) Multi-factor authentication is mandatory for all remote access

c) Privileged access requires executive approval and quarterly review

d) Access credentials must be unique to each individual

2. Network Segmentation

a) ICS networks must maintain physical or logical separation from enterprise IT networks

b) Implementation of DMZs between security zones is mandatory

c) Network segmentation must align with the Company's Zone-Conduit model

4. Security Monitoring and Incident Response

1. Continuous Monitoring

a) All ICS networks shall be monitored 24/7 using Company's AI-driven detection systems

b) Baseline behavior profiles must be established and maintained for all critical systems

c) Anomaly detection thresholds shall be reviewed monthly

2. Incident Response

a) Security incidents must be reported to the Security Operations Center within 30 minutes

b) Incident response procedures shall be tested quarterly

c) Post-incident analysis reports are required within 48 hours

5. Configuration Management

1. System Hardening

a) All ICS components must be configured according to Company-approved security baselines

b) Default passwords must be changed before deployment

c) Unnecessary services and ports must be disabled

2. Change Management

a) All changes require documented approval through the Change Advisory Board

b) Emergency changes must be logged and reviewed within 24 hours

c) Configuration backups are required before and after changes

6. Risk Assessment and Compliance

1. Risk Assessments

a) Comprehensive risk assessments must be conducted annually

b) Vulnerability scanning must be performed quarterly using approved tools

c) Third-party security audits are required every 18 months

2. Compliance Requirements

a) All systems must maintain compliance with relevant industry standards

b) Documentation of compliance must be maintained and updated quarterly

c) Non-compliance issues must be remediated within 30 days

7. Training and Awareness

1. All personnel with ICS access must complete:

a) Initial security awareness training

b) Annual refresher training

c) Role-specific technical training

d) Quarterly security updates

8. Documentation and Record Keeping

1. Required Documentation

a) System architecture diagrams

b) Network topology maps

c) Asset inventory lists

d) Security incident reports

e) Training records

2. Retention Requirements

a) All security-related documentation must be retained for 5 years

b) Audit logs must be retained for 3 years

c) Incident reports must be retained for 7 years

9. Enforcement and Exceptions

1. Violations of these Guidelines may result in disciplinary action up to and including termination of employment or service agreement.

2. Exceptions to these Guidelines must be:

a) Documented in writing

b) Approved by the Chief Security Architect

c) Reviewed annually

d) Limited in duration to no more than 12 months

10. Review and Updates

1. These Guidelines shall be reviewed and updated annually or upon significant changes to:

a) Technology infrastructure

b) Threat landscape

c) Regulatory requirements

d) Business operations

Approved by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: _

Document Control Number: ICS-SEC-2024-001