Industrial Network Security Compliance Checklist

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document Reference: DSS-SEC-2024-001

1. Purpose and Scope

1. This Industrial Network Security Compliance Checklist ("Checklist") establishes the mandatory security controls and compliance requirements for all industrial control system (ICS) environments protected by DeepShield Systems, Inc. ("DeepShield") solutions.

2. This Checklist applies to all DeepShield products, services, and implementations involving operational technology (OT) networks, SCADA systems, and industrial automation infrastructure.

2. Network Architecture Security Requirements

1. Network Segmentation

- Implementation of minimum three-tier network architecture
- Physical separation between IT and OT networks
- Dedicated DMZ for data exchange between zones
- Documented network topology with clear security boundaries

2. Access Control

- Role-based access control (RBAC) implementation
- Multi-factor authentication for all privileged access
- Separate authentication domains for IT and OT systems
- Regular access rights review and certification

3. Communication Security

- Encrypted protocols for all inter-zone communication
- Whitelisting of authorized protocols and ports
- Implementation of unidirectional security gateways where applicable
- Regular validation of communication patterns

3. System Hardening Requirements

1. Industrial Control Systems

- Removal of unnecessary services and applications
- Implementation of secure configurations
- Regular firmware updates and patch management
- Baseline security configuration documentation

2. Network Devices

- Password complexity requirements
- Disabled unused ports and services
- Secure management protocols
- Logging and monitoring configuration

3. Endpoints and HMIs

- Application whitelisting
- USB port control
- Screen lock requirements
- Local firewall configuration

4. Monitoring and Detection Requirements

1. Security Information and Event Management

- Real-time monitoring of all security events
- Correlation of IT and OT security alerts
- Automated anomaly detection
- Retention of security logs for minimum 12 months

2. Asset Management

- Continuous asset discovery and inventory
- Baseline behavior profiling
- Change detection and management
- Asset vulnerability assessment

5. Incident Response and Recovery

1. Response Procedures

- Documented incident response plan
- Defined escalation procedures
- Communication protocols
- Regular testing and updates of response procedures

2. Business Continuity

- Backup and recovery procedures
- System restoration priorities
- Alternative operation procedures
- Regular disaster recovery testing

6. Compliance Documentation Requirements

1. Required Documentation

- Network architecture diagrams
- Asset inventory records
- Security control implementations
- Risk assessment reports
- Incident response procedures
- Training records

2. Review and Updates

- Quarterly review of security controls
- Annual compliance assessment
- Documentation version control
- Change management records

7. Audit and Assessment

1. Internal Audits

- Quarterly security control assessments
- Monthly compliance reviews
- Regular penetration testing

- Vulnerability scanning

2. External Audits

- Annual third-party security assessment
- Regulatory compliance validation
- Industry certification maintenance
- Independent penetration testing

8. Compliance Verification

The undersigned certifies that all requirements specified in this Checklist have been reviewed and implemented according to DeepShield Systems' security standards and applicable regulatory requirements.

```

**Compliance Officer: _**

**Date:**

**Security Director:**

**Date:**

**Chief Technology Officer: _**

**Date:**

```

9. Legal Disclaimer

This Checklist is confidential and proprietary to DeepShield Systems, Inc. It contains sensitive security information and shall not be disclosed to unauthorized parties. DeepShield Systems reserves the right to modify this Checklist at any time. Compliance with this Checklist does not guarantee complete security or regulatory compliance. Users must ensure compliance with all applicable laws and regulations.

End of Document