Operational Technology Security Guidelines v2.4

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Control #: OT-SEC-2024-001

1. Purpose and Scope

1. These Operational Technology Security Guidelines ("Guidelines") establish the mandatory security requirements and controls for all operational technology ("OT") environments, industrial control systems ("ICS"), and critical infrastructure protection measures within DeepShield Systems, Inc. ("Company") and its client deployments.

2. These Guidelines apply to all Company employees, contractors, consultants, temporary workers, and other business partners who interact with or support OT environments.

2. Definitions

1. "Operational Technology (OT)" refers to hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in industrial environments.

2. "Critical Infrastructure" means systems and assets, whether physical or virtual, so vital that their incapacity or destruction would have a debilitating impact on security, economic security, public health or safety, or any combination thereof.

3. "Security Architecture" refers to DeepShield's proprietary deep-layer security framework incorporating AI-driven threat detection, real-time monitoring, and adaptive defense mechanisms.

3. Security Controls and Requirements

1. Network Segmentation

a) All OT networks must maintain strict separation from enterprise IT networks through physical or logical segmentation

b) Implementation of DMZ architecture for any required IT-OT communication

c) Minimum of three network security zones: Enterprise, DMZ, and OT

d) Regular validation of segmentation effectiveness through penetration testing

2. Access Control

a) Implementation of role-based access control (RBAC)

b) Multi-factor authentication for all remote access

c) Privileged Access Management (PAM) for administrative functions

d) Regular access rights review and certification

3. Security Monitoring

a) Continuous monitoring of OT network traffic

b) Implementation of anomaly detection systems

c) Security Information and Event Management (SIEM) integration

d) 24/7 Security Operations Center (SOC) coverage

4. Incident Response and Recovery

1. Incident Classification

a) Level 1 - Minor operational disruption

b) Level 2 - Significant system compromise

c) Level 3 - Critical infrastructure impact

d) Level 4 - Catastrophic system failure

2. Response Procedures

a) Immediate containment measures

b) Evidence preservation

c) Root cause analysis

d) Stakeholder notification

e) Recovery and restoration

5. Compliance and Audit

1. Regular compliance assessments against:

a) NIST Cybersecurity Framework

b) IEC 62443 Standards

c) NERC CIP Requirements

d) Company-specific security standards

2. Audit Requirements

a) Annual third-party security audits

b) Quarterly internal assessments

c) Monthly vulnerability scanning

d) Continuous compliance monitoring

6. Training and Awareness

1. Required Training Programs

a) Initial OT security orientation

b) Annual security awareness refresher

c) Role-specific technical training

d) Incident response drills

7. Documentation and Record Keeping

1. Mandatory Documentation

a) System architecture diagrams

b) Network topology maps

c) Asset inventory

d) Configuration baselines

e) Change management records

2. Retention Requirements

a) Security incident reports: 7 years

b) Audit logs: 3 years

c) Access control records: 5 years

d) Training records: 3 years

8. Review and Updates

1. These Guidelines shall be reviewed and updated:

a) Annually at minimum

b) Following major security incidents

c) Upon significant technology changes

d) As required by regulatory changes

9. Legal Compliance and Liability

1. These Guidelines are designed to comply with all applicable laws and regulations but do not guarantee compliance. The Company reserves the right to modify these Guidelines at any time.

2. Nothing in these Guidelines shall be construed to create any contractual or other legal rights.

Approval and Authorization

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Marcus Chen

Chief Executive Officer

Date: January 15, 2024

By:

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024

Document Version History:

v2.4 - January 15, 2024

v2.3 - July 1, 2023

v2.2 - January 10, 2023

v2.1 - June 15, 2022

v2.0 - January 1, 2022