VESSEL NETWORK SECURITY REQUIREMENTS

DeepShield Systems, Inc.

Document Version: 2.4

Effective Date: January 15, 2024

1. PURPOSE AND SCOPE

1. This document establishes mandatory network security requirements for all vessels utilizing DeepShield Systems, Inc. ("DeepShield") cybersecurity solutions and infrastructure protection systems.

2. These requirements apply to all maritime vessels, offshore platforms, and floating facilities that implement or interface with DeepShield's OT security architecture, including but not limited to:

a) Commercial shipping vessels

b) Offshore energy platforms

c) Maritime industrial facilities

d) Subsea infrastructure control systems

e) Port facility operations networks

2. DEFINITIONS

1. "Critical OT Systems" means operational technology systems essential for vessel navigation, propulsion, safety, or cargo operations.

2. "Security Zone" means a logically or physically isolated network segment with defined security controls and access restrictions.

3. "DeepShield Platform" means the company's proprietary industrial cybersecurity solution including all associated hardware, software, and monitoring systems.

3. NETWORK ARCHITECTURE REQUIREMENTS

1. Network Segmentation

a) Minimum of three (3) distinct security zones for: (i) IT systems, (ii) OT systems, and (iii) critical safety systems

b) Physical or logical separation between zones using approved firewalls or data diodes

c) Implementation of DeepShield's Zone-Lock(TM) technology for inter-zone communications

2. Access Controls

a) Role-based access control (RBAC) for all network resources

b) Multi-factor authentication for administrative access

c) Separate authentication domains for each security zone

d) Automated access logging and review procedures

4. SECURITY MONITORING AND RESPONSE

1. Continuous Monitoring Requirements

a) Real-time network traffic analysis using DeepShield sensors

b) Automated anomaly detection and alerting

c) Asset inventory and configuration monitoring

d) Security log collection and correlation

2. Incident Response Procedures

a) Maintained incident response plan with defined roles

b) 24/7 monitoring and response capability

c) Automated containment procedures for identified threats

d) Mandatory incident reporting within specified timeframes

5. TECHNICAL CONTROLS

1. Encryption Requirements

a) AES-256 encryption for all critical data transmission

b) TLS 1.3 or higher for external communications

c) Hardware security modules for key storage

d) Regular encryption key rotation procedures

2. System Hardening

a) Removal of unnecessary services and applications

b) Regular security patches and updates

c) Secure configuration baselines

d) Physical security controls for network equipment

6. COMPLIANCE AND AUDITING

1. Compliance Requirements

a) Annual security assessments

b) Quarterly vulnerability scanning

c) Monthly configuration reviews

d) Continuous compliance monitoring

2. Documentation Requirements

a) Updated network diagrams

b) Security control inventory

c) Risk assessment reports

d) Incident response records

7. MAINTENANCE AND UPDATES

1. System maintenance shall be performed according to DeepShield's prescribed schedules and procedures.

2. Security updates must be applied within:

a) 24 hours for critical vulnerabilities

b) 72 hours for high-risk vulnerabilities

c) 7 days for medium-risk vulnerabilities

d) 30 days for low-risk vulnerabilities

8. LIABILITY AND ENFORCEMENT

1. Compliance with these requirements is mandatory for maintaining DeepShield support and warranty coverage.

2. DeepShield reserves the right to suspend services for non-compliant vessels until remediation is completed.

9. MODIFICATIONS AND UPDATES

1. DeepShield may modify these requirements with 30 days' written notice to vessel operators.

2. Emergency security requirements may be implemented immediately upon notification.

ACKNOWLEDGMENT

The undersigned acknowledges receipt and acceptance of these Vessel Network Security Requirements:

Vessel Operator: _

Authorized Representative: _

Title: _

Date: _

DeepShield Systems, Inc.

By: _

Title: _

Date: _

End of Document