VESSEL NETWORK PROTECTION PROTOCOL

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Vessel Network Protection Protocol ("Protocol") establishes mandatory security requirements and operational procedures for the protection of maritime vessel networks utilizing DeepShield Systems, Inc.'s ("DeepShield") industrial control system (ICS) security solutions.

2. This Protocol applies to all vessel network implementations incorporating DeepShield's Maritime Defense Platform(TM) and associated subsystems for operational technology (OT) protection.

2. DEFINITIONS

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

2. "Maritime Defense Platform" means DeepShield's proprietary vessel network security solution comprising hardware components, software systems, and AI-driven monitoring capabilities.

3. "Security Event" means any detected or suspected unauthorized access, anomalous behavior, or cyber threat affecting protected vessel networks.

4. "Vessel Network" means the complete operational technology infrastructure aboard a maritime vessel, including all connected industrial control systems, SCADA components, and automation elements.

3. IMPLEMENTATION REQUIREMENTS

1. Network Segmentation

1.1. All vessel networks must maintain strict separation between operational technology (OT) and information technology (IT) environments through DeepShield's proprietary OT-Secure(TM) architecture.

1.2. Critical Systems must operate on isolated network segments with dedicated security controls and monitoring.

2. Access Control

2.1. Multi-factor authentication is required for all administrative access to vessel network components.

2.2. Role-based access control (RBAC) must be implemented according to DeepShield's Maritime Access Matrix(TM).

3. Monitoring and Detection

3.1. Continuous real-time monitoring of all network traffic using DeepShield's AI-driven anomaly detection system.

3.2. Automated asset discovery and inventory maintenance with hourly updates to the secure configuration database.

4. SECURITY PROTOCOLS

1. Threat Response

1.1. Automated incident response procedures shall be activated upon detection of Security Events according to DeepShield's Maritime Threat Response Framework(TM).

1.2. Security Events shall be classified and handled according to the following severity levels:

- Level 1: Informational
- Level 2: Warning
- Level 3: Critical
- Level 4: Emergency

2. System Updates

2.1. Security updates to the Maritime Defense Platform shall be deployed through DeepShield's secure OTA update mechanism.

2.2. All updates must be cryptographically signed and verified before installation.

5. COMPLIANCE AND REPORTING

1. Audit Requirements

1.1. Monthly security audits of vessel network configurations and access logs.

1.2. Quarterly penetration testing of Critical Systems by DeepShield-certified security professionals.

2. Documentation

2.1. Maintenance of detailed security event logs for a minimum of 365 days.

2.2. Generation of compliance reports according to IMO Cybersecurity Guidelines and applicable maritime regulations.

6. INCIDENT MANAGEMENT

1. Response Procedures

1.1. Security Events classified as Level 3 or 4 require immediate notification to DeepShield's Maritime Security Operations Center (MSOC).

1.2. Incident response teams must be activated within 15 minutes of critical alert detection.

2. Recovery Operations

2.1. System restoration procedures must follow DeepShield's Maritime Recovery Protocol(TM).

2.2. Post-incident analysis reports required within 48 hours of incident resolution.

7. LIMITATIONS OF LIABILITY

1. DeepShield Systems, Inc. shall not be liable for any consequential, incidental, or indirect damages arising from the implementation of this Protocol or the use of the Maritime Defense Platform.

2. This Protocol does not guarantee complete protection against all cyber threats or network vulnerabilities.

8. MODIFICATION AND GOVERNANCE

1. This Protocol may be modified by DeepShield Systems, Inc. with 30 days written notice to affected parties.

2. The DeepShield Maritime Security Council shall oversee the maintenance and updates to this

Protocol.

EXECUTION

IN WITNESS WHEREOF, the undersigned acknowledges and agrees to implement this Vessel Network Protection Protocol.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: