MARITIME CYBERSECURITY TRAINING MANUAL

DeepShield Systems, Inc.

Version 3.2 - January 2024

Document Control #: DSS-MTM-2024-01

1. INTRODUCTION AND SCOPE

1. This Maritime Cybersecurity Training Manual ("Manual") establishes mandatory training requirements and procedures for all personnel involved in maritime operations utilizing DeepShield Systems, Inc. ("DeepShield") cybersecurity solutions and platforms.

2. This Manual is considered confidential and proprietary to DeepShield Systems, Inc. and is subject to the terms of applicable Non-Disclosure Agreements.

2. DEFINITIONS

1. "Critical Maritime Systems" means any operational technology (OT) systems, industrial control systems (ICS), or network infrastructure deployed in maritime environments.

2. "Qualified Personnel" refers to individuals who have completed DeepShield's Maritime Cybersecurity Certification Program.

3. "Security Incident" means any actual or suspected compromise, unauthorized access, or anomalous activity affecting Critical Maritime Systems.

3. TRAINING REQUIREMENTS

1. Mandatory Training Modules

- Module A: Maritime OT Architecture & Attack Vectors
- Module B: DeepShield Maritime Defense Platform Operations
- Module C: Incident Response Protocols
- Module D: Compliance & Regulatory Requirements
- Module E: Advanced Threat Detection & Mitigation

2. Certification Requirements

a) All personnel must complete initial certification within 60 days of assignment

b) Annual recertification required for continued system access

c) Additional certification required for specialized maritime modules

3. Documentation Requirements

a) Training completion records maintained for 5 years

b) Certification status tracked in DeepShield's Compliance Management System

c) Quarterly reports generated for regulatory compliance

4. OPERATIONAL PROCEDURES

1. System Access Controls

a) Two-factor authentication required for all system access

b) Biometric verification for critical system modifications

c) Role-based access control (RBAC) implementation

d) Regular access review and audit procedures

2. Incident Response Protocols

a) Immediate notification to Maritime Security Operations Center

b) Implementation of containment procedures

c) Evidence preservation requirements

d) Regulatory reporting obligations

e) Post-incident analysis and documentation

5. COMPLIANCE AND AUDIT

1. Regulatory Standards

- IMO Guidelines on Maritime Cyber Risk Management
- NIST Cybersecurity Framework
- BIMCO Guidelines on Cyber Security
- ISO/IEC 27001 Information Security Management

2. Audit Requirements

a) Quarterly internal audits of training compliance

b) Annual third-party certification review

c) Random spot checks of operational procedures

d) Documentation retention requirements

6. SECURITY PROTOCOLS

1. Network Segmentation

a) Physical separation of operational and corporate networks

b) DMZ implementation requirements

c) Secure remote access procedures

2. Threat Monitoring

a) 24/7 Security Operations Center (SOC) monitoring

b) AI-driven anomaly detection

c) Real-time threat intelligence integration

d) Automated response capabilities

7. LIABILITY AND INDEMNIFICATION

1. DeepShield Systems, Inc. shall not be liable for any damages arising from:

a) Failure to follow training procedures

b) Unauthorized system modifications

c) Delayed incident reporting

d) Non-compliance with certification requirements

2. Customer obligations include:

a) Maintaining current certification status

b) Prompt reporting of security incidents

c) Compliance with all training requirements

d) Documentation of operational procedures

8. AMENDMENTS AND UPDATES

1. DeepShield reserves the right to modify this Manual as necessary to address:

a) Emerging security threats

b) Regulatory changes

c) Technology updates

d) Operational requirements

2. Notice of material changes will be provided 30 days prior to implementation.

9. EXECUTION

This Manual is effective as of January 15, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

Date:

APPROVED:

By:

Sarah Blackwood

Chief Technology Officer

Date:

End of Document