Maritime IoT Device Security Standards

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: Confidential

1. Purpose and Scope

1. This document establishes mandatory security standards and compliance requirements for all Internet of Things (IoT) devices deployed in maritime environments under DeepShield Systems, Inc.'s ("DeepShield") operational purview.

2. These standards apply to all IoT devices, sensors, and connected equipment utilized in:

a) Vessel operational technology (OT) systems

b) Port facility infrastructure

c) Offshore platform monitoring systems

d) Maritime cargo tracking systems

e) Navigation and positioning equipment

2. Definitions

1. "Maritime IoT Device" means any network-connected device, sensor, or equipment deployed in maritime operational environments that collects, transmits, or processes data related to maritime operations.

2. "Security Architecture" refers to DeepShield's proprietary deep-layer security framework incorporating AI-driven threat detection and response capabilities.

3. "Critical Systems" means any IoT devices or systems whose compromise could impact vessel safety, navigation, or critical operations.

3. Device Security Requirements

1. Authentication and Access Control

a) All devices must implement multi-factor authentication

b) Unique device identifiers and certificates must be assigned

c) Role-based access control (RBAC) must be enforced

d) Default passwords must be changed before deployment

2. Encryption Standards

a) AES-256 encryption required for data at rest

b) TLS 1.3 or higher required for data in transit

c) Hardware security modules (HSM) required for critical systems

d) Secure key management system integration mandatory

3. Network Security

a) Network segmentation requirements

b) Firewall and intrusion detection system integration

c) Regular vulnerability scanning

d) Secure boot verification

4. Monitoring and Incident Response

1. All maritime IoT devices must integrate with DeepShield's central monitoring system for:

a) Real-time threat detection

b) Anomaly identification

c) Performance monitoring

d) Security event logging

2. Incident Response Protocols

a) Automated threat containment

b) Incident escalation procedures

c) Recovery and rollback capabilities

d) Forensic data collection

5. Compliance and Testing

1. Pre-deployment Testing

a) Security architecture validation

b) Penetration testing requirements

c) Compliance verification

d) Performance benchmarking

2. Ongoing Compliance

a) Quarterly security assessments

b) Annual certification renewal

c) Compliance documentation

d) Audit trail maintenance

6. Update and Patch Management

1. All maritime IoT devices must maintain:

a) Automated patch management capabilities

b) Secure update mechanisms

c) Version control systems

d) Rollback capabilities

2. Update Schedule Requirements

a) Critical updates within 24 hours

b) Security patches within 72 hours

c) Feature updates quarterly

d) Documentation updates monthly

7. Documentation Requirements

1. Required Documentation

a) Device security specifications

b) Network architecture diagrams

c) Risk assessment reports

d) Compliance certificates

2. Maintenance Records

a) Update history

b) Incident reports

c) Performance metrics

d) Security audit logs

8. Liability and Indemnification

1. DeepShield maintains no liability for security incidents resulting from:

a) Unauthorized device modifications

b) Failure to implement required security measures

c) Non-compliance with these standards

d) Third-party component vulnerabilities

9. Amendments and Updates

1. DeepShield reserves the right to modify these standards as necessary to maintain security effectiveness and regulatory compliance.

2. Notification of changes will be provided 30 days prior to implementation unless immediate security concerns require faster deployment.

10. Execution and Acknowledgment

IN WITNESS WHEREOF, the undersigned acknowledges and agrees to comply with these Maritime IoT Device Security Standards.

DeepShield Systems, Inc.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date:

Approved:

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: