IMO Cybersecurity Guidelines Implementation Plan

DOCUMENT ID: DSS-IMO-CY-2024-001

EFFECTIVE DATE: January 15, 2024

VERSION: 1.0

CLASSIFICATION: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Implementation Plan ("Plan") establishes DeepShield Systems, Inc.'s ("DeepShield") framework for implementing the International Maritime Organization's ("IMO") Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) and Resolution MSC.428(98) across its maritime cybersecurity solutions and services.

2. This Plan applies to all DeepShield maritime cybersecurity products, services, and operations that interface with or support vessels subject to the International Convention for the Safety of Life at Sea (SOLAS).

2. DEFINITIONS

1. "IMO Guidelines" refers to the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) and associated IMO cybersecurity regulations.

2. "Maritime Systems" means all DeepShield products and services designed for maritime applications, including but not limited to the DeepShield Maritime Defense Suite(TM), OceanGuard(TM) platform, and associated subsea protection modules.

3. "Implementation Period" means the 12-month period following the Effective Date of this Plan.

3. COMPLIANCE REQUIREMENTS

1. Risk Assessment and Management

- Conduct comprehensive cyber risk assessments for all Maritime Systems
- Document threat modeling specific to maritime operational technology environments
- Implement risk mitigation controls aligned with IMO Guidelines
- Maintain risk registers and review quarterly

2. Technical Controls

- Deploy maritime-specific intrusion detection systems
- Implement network segmentation for vessel operational technology
- Establish secure remote access protocols for offshore systems
- Configure automated threat response mechanisms

3. Documentation and Reporting

- Maintain detailed implementation records
- Generate quarterly compliance reports
- Document all security incidents and remediation actions
- Prepare annual attestation of IMO Guidelines compliance

4. IMPLEMENTATION SCHEDULE

1. Phase 1 (Months 1-3)

- Review existing maritime cybersecurity controls
- Gap analysis against IMO Guidelines
- Development of maritime-specific security policies
- Initial staff training on IMO requirements

2. Phase 2 (Months 4-7)

- Technical control implementation
- Security monitoring system deployment
- Documentation system establishment
- Vendor compliance verification

3. Phase 3 (Months 8-12)

- Testing and validation
- Compliance verification
- Final documentation
- Certification preparation

5. ROLES AND RESPONSIBILITIES

1. Chief Security Architect

- Overall implementation oversight
- Technical architecture approval
- Final compliance verification

2. Maritime Security Team

- Day-to-day implementation activities
- Technical control deployment
- Documentation maintenance
- Training delivery

3. Compliance Officer

- Regulatory alignment verification
- Audit coordination
- Reporting oversight
- Documentation review

6. MONITORING AND REVIEW

1. Implementation Monitoring

- Weekly progress reviews
- Monthly status reports
- Quarterly compliance assessments
- Annual comprehensive review

2. Performance Metrics

- Implementation milestone completion
- Security incident metrics
- Compliance violation tracking
- Response time measurements

7. AMENDMENTS AND UPDATES

1. This Plan shall be reviewed and updated annually or upon significant changes to IMO Guidelines or maritime cybersecurity requirements.

2. All amendments must be approved by DeepShield's Chief Security Architect and documented in the version control system.

8. CONFIDENTIALITY

1. This document contains confidential and proprietary information of DeepShield Systems, Inc. and shall not be disclosed to third parties without written authorization.

9. APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Implementation Plan has been approved and executed by the undersigned authorized representatives of DeepShield Systems, Inc.

APPROVED BY:

Dr. Elena Rodriguez
Chief Security Architect
Date: January 15, 2024

Sarah Blackwood
Chief Technology Officer
Date: January 15, 2024

James Morrison
VP of Engineering
Date: January 15, 2024