RISK MANAGEMENT FRAMEWORK DOCUMENTATION

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document Version: 3.2

Classification: Confidential

1. INTRODUCTION

1. This Risk Management Framework ("Framework") establishes the comprehensive approach to risk identification, assessment, and mitigation for DeepShield Systems, Inc. ("Company") in relation to its industrial cybersecurity and critical infrastructure protection operations.

2. This Framework has been approved by the Board of Directors and is subject to annual review by the Risk Management Committee.

2. SCOPE AND APPLICABILITY

1. This Framework applies to all Company operations, including:

a) Industrial Control System (ICS) security solutions

b) SCADA network protection services

c) Maritime and subsea infrastructure security

d) Operational Technology (OT) environment monitoring

e) AI-driven threat detection systems

2. Geographic Coverage: All Company operations within North America, Europe, Asia-Pacific, and adjacent maritime territories.

3. RISK GOVERNANCE STRUCTURE

1. Board Risk Committee

- Quarterly review of enterprise risk profile
- Approval of risk tolerance thresholds
- Oversight of risk management effectiveness

2. Executive Risk Management Team

- Chief Risk Officer (reporting to CEO)
- Chief Security Architect
- VP of Engineering
- Chief Compliance Officer
- General Counsel

3. Operational Risk Units
- Product Security Team
- Client Implementation Risk Team
- Infrastructure Protection Unit
- Maritime Operations Risk Team

4. RISK ASSESSMENT METHODOLOGY

1. Risk Categories
- Technical Security Risks
- Operational Technology Risks
- Client Implementation Risks
- Regulatory Compliance Risks
- Third-Party Vendor Risks
- Maritime Infrastructure Risks

2. Risk Assessment Process

a) Initial Risk Identification

b) Impact Analysis

c) Probability Assessment

d) Risk Rating Assignment

e) Control Effectiveness Evaluation

f) Residual Risk Determination

3. Risk Rating Matrix
- Critical (Score 15-25)
- High (Score 10-14)

- Medium (Score 5-9)
- Low (Score 1-4)

5. CONTROL FRAMEWORK

1. Technical Controls

- AI-Based Threat Detection Systems
- Real-Time Monitoring Protocols
- Automated Incident Response Mechanisms
- Deep-Layer Security Architecture
- Maritime-Specific Security Controls

2. Operational Controls

- Change Management Procedures
- Access Control Protocols
- Incident Response Plans
- Business Continuity Measures
- Disaster Recovery Procedures

3. Administrative Controls

- Policy Framework
- Training Requirements
- Documentation Standards
- Audit Procedures
- Compliance Monitoring

6. MONITORING AND REPORTING

1. Key Risk Indicators (KRIs)

- System Availability Metrics
- Security Incident Rates
- Client Implementation Success Rates
- Regulatory Compliance Scores
- Third-Party Risk Ratings

2. Reporting Requirements

- Monthly Risk Dashboard
- Quarterly Risk Committee Reports
- Annual Risk Assessment Review
- Incident Response Reports
- Regulatory Compliance Reports

7. REVIEW AND UPDATES

1. Framework Review Schedule

- Annual comprehensive review
- Quarterly control effectiveness assessment
- Monthly KRI review
- Ad-hoc updates as required

2. Change Management Process

- Documentation of proposed changes
- Impact assessment
- Approval requirements
- Implementation timeline
- Communication plan

8. COMPLIANCE AND REGULATORY REQUIREMENTS

1. Regulatory Framework Alignment

- NIST Cybersecurity Framework
- ISO 27001 Requirements
- Maritime Cybersecurity Guidelines
- Industry-Specific Standards
- Regional Regulatory Requirements

9. ATTESTATION

This Framework has been reviewed and approved by the Board of Directors of DeepShield Systems,

Inc.

APPROVED BY:

Dr. Marcus Chen

Chief Executive Officer

Date: January 11, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 11, 2024

Robert Kessler

Chief Financial Officer

Date: January 11, 2024

10. LEGAL DISCLAIMER

This document contains confidential and proprietary information of DeepShield Systems, Inc. No part of this document may be reproduced, stored, or transmitted without prior written permission. This Framework is subject to change without notice and does not constitute a binding obligation on the part of the Company.