THIRD-PARTY RISK ASSESSMENT FRAMEWORK

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Third-Party Risk Assessment Framework ("Framework") establishes the standardized methodology and requirements for evaluating, monitoring, and managing risks associated with third-party vendors, suppliers, contractors, and service providers (collectively "Third Parties") engaged by DeepShield Systems, Inc. ("Company").

2. This Framework applies to all Third Parties that:

a) Access, process, store, or transmit Company data

b) Interface with Company's industrial control systems (ICS)

c) Provide critical components or services for the Company's security platform

d) Have physical or logical access to Company facilities or networks

e) Provide services related to maritime or subsea infrastructure protection

2. RISK CLASSIFICATION TIERS

1. Third Parties shall be classified into the following risk tiers:

Tier 1 (Critical)

- Direct access to ICS environments
- Access to SCADA networks
- Maritime security system components
- Core platform infrastructure services

Tier 2 (High)

- Indirect access to operational technology
- Non-critical platform components
- Secondary security services

- Data processing services

Tier 3 (Moderate)

- Administrative services
- Non-technical vendors
- General support services

3. ASSESSMENT REQUIREMENTS

1. Initial Assessment

- Security capabilities evaluation
- Technical architecture review
- Compliance certification verification
- Financial stability analysis
- Insurance coverage validation
- Business continuity assessment
- Data protection controls review

2. Periodic Reassessment

- Tier 1: Every 6 months
- Tier 2: Annual
- Tier 3: Every 24 months

4. SECURITY AND COMPLIANCE STANDARDS

1. All Third Parties must demonstrate compliance with:

- ISO 27001 Information Security Management
- IEC 62443 Industrial Network Security
- NIST Cybersecurity Framework
- Maritime cybersecurity regulations (where applicable)

2. Additional Requirements for Tier 1 Vendors:

- SOC 2 Type II certification
- Penetration testing results

- Vulnerability management program
- 24/7 security monitoring
- Incident response capabilities

5. CONTRACTUAL REQUIREMENTS

1. All Third Party agreements must include:

- Security requirements and standards
- Data protection obligations
- Audit rights and access
- Incident reporting procedures
- Service level agreements
- Termination provisions
- Insurance requirements
- Indemnification clauses

6. MONITORING AND OVERSIGHT

1. Continuous Monitoring

- Security posture assessment
- Performance metrics tracking
- Compliance verification
- Risk indicator monitoring
- Service level agreement compliance

2. Incident Management

- Mandatory breach notification
- Investigation cooperation
- Root cause analysis
- Remediation requirements
- Impact assessment

7. RISK MITIGATION MEASURES

1. Required Controls

- Access management protocols
- Encryption requirements
- Network segmentation
- Authentication standards
- Audit logging
- Change management procedures

2. Contingency Planning

- Business continuity requirements
- Disaster recovery capabilities
- Backup procedures
- Alternative provider arrangements

8. GOVERNANCE AND REPORTING

1. Oversight Structure

- Third Party Risk Committee
- Security Review Board
- Compliance Team
- Technical Assessment Team

2. Reporting Requirements

- Quarterly risk assessments
- Annual compliance reports
- Security incident reports
- Performance metrics
- Audit findings

9. ENFORCEMENT AND EXCEPTIONS

1. Non-compliance may result in:

- Immediate service suspension
- Contract termination

- Financial penalties
- Legal action

2. Exceptions require:

- Written justification
- Risk assessment
- Compensating controls
- Executive approval
- Regular review

10. DOCUMENT CONTROL

Version: 2.0

Approved By: Security Review Board

Date: January 15, 2024

Next Review: January 15, 2025

AUTHORIZATION

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Marcus Chen

Chief Executive Officer

By:

Sarah Blackwood

Chief Technology Officer

By:

Dr. Elena Rodriguez

Chief Security Architect