RISK MANAGEMENT FRAMEWORK

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

1. PURPOSE AND SCOPE

1. This Risk Management Framework ("Framework") establishes the comprehensive approach to identifying, assessing, and mitigating risks across DeepShield Systems, Inc.'s ("Company") operations, with particular focus on industrial cybersecurity solutions and critical infrastructure protection services.

2. This Framework applies to all Company operations, employees, contractors, and third-party service providers involved in the development, deployment, and maintenance of the Company's industrial control system (ICS) security solutions.

2. DEFINITIONS

1. "Critical Risk" means any risk that could result in severe disruption to customer operations, compromise of industrial control systems, or breach of operational technology environments.

2. "Risk Owner" refers to the designated executive or senior manager responsible for overseeing specific risk categories and implementing mitigation strategies.

3. "Risk Register" means the centralized database maintaining documentation of identified risks, their assessment, and mitigation measures.

3. RISK GOVERNANCE STRUCTURE

1. Board Risk Committee

- Oversees enterprise-wide risk management strategy
- Reviews quarterly risk assessments and mitigation effectiveness
- Approves risk tolerance levels and major risk management policies

2. Executive Risk Management Committee

- Chaired by Chief Security Architect

- Meets monthly to review operational risk metrics
- Coordinates cross-functional risk response initiatives

3. Operational Risk Teams

- Technology Risk Team (Led by CTO)
- Product Security Team (Led by VP of Engineering)
- Customer Implementation Risk Team (Led by VP of Professional Services)

4. RISK ASSESSMENT METHODOLOGY

1. Risk Identification

- Continuous monitoring of threat landscape
- Regular security audits of ICS implementations
- Customer environment vulnerability assessments
- Supply chain risk evaluation
- Emerging technology risk analysis

2. Risk Assessment Criteria

- Impact severity (1-5 scale)
- Probability of occurrence
- Detection capability
- Time to impact
- Financial implications
- Reputational impact

3. Risk Categorization

- Technical risks
- Operational risks
- Strategic risks
- Compliance risks
- Financial risks

5. RISK MITIGATION AND CONTROL

1. Required Control Categories

- Preventive controls
- Detective controls
- Corrective controls
- Compensating controls

2. Mitigation Strategy Requirements

- Documented mitigation plan for all High and Critical risks
- Quarterly review of mitigation effectiveness
- Resource allocation for risk treatment
- Implementation timeline and milestones
- Success metrics and KPIs

6. MONITORING AND REPORTING

1. Regular Monitoring Activities

- Real-time monitoring of critical system components
- Weekly review of security incidents
- Monthly risk metric dashboard updates
- Quarterly compliance assessments

2. Reporting Requirements

- Monthly risk status reports to Executive Committee
- Quarterly risk reviews with Board Risk Committee
- Annual comprehensive risk assessment report
- Immediate notification of Critical Risk events

7. INCIDENT RESPONSE AND ESCALATION

1. Incident Classification

- Severity levels (1-4)
- Response time requirements
- Escalation triggers
- Communication protocols

2. Escalation Procedures

- Technical escalation path
- Management escalation path
- Customer notification requirements
- Regulatory reporting obligations

8. COMPLIANCE AND REVIEW

1. Framework Review

- Annual review of Framework effectiveness
- Updates based on emerging threats and industry standards
- Integration with ISO 27001 and IEC 62443 requirements
- Alignment with customer compliance requirements

2. Documentation Requirements

- Maintenance of risk assessment records
- Control testing evidence
- Incident response documentation
- Audit trails of risk decisions

9. TRAINING AND AWARENESS

1. Required Training

- Annual risk management training for all employees
- Quarterly updates for risk owners
- Role-specific security awareness training
- Incident response drills

10. SIGNATURE AND APPROVAL

APPROVED AND ADOPTED by the Board of Directors of DeepShield Systems, Inc.

Date: January 15, 2024

_

Dr. Marcus Chen

Chief Executive Officer

_

Dr. Elena Rodriguez

Chief Security Architect

_

Robert Kessler

Chief Financial Officer