THIRD-PARTY RISK ASSESSMENT DOCUMENTATION

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document Reference: TPRA-2024-001

1. PURPOSE AND SCOPE

1. This Third-Party Risk Assessment Documentation ("Documentation") establishes the formal procedures 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 Documentation applies to all Third Parties that:

a) Have access to Company systems, networks, or data

b) Provide critical components or services for the Company's industrial cybersecurity platform

c) Interface with the Company's customer environments

d) Support mission-critical operations

2. RISK ASSESSMENT FRAMEWORK

1. Risk Classification Tiers:

- Tier 1: Critical (Direct access to OT systems or customer environments)
- Tier 2: High (Access to sensitive data or core systems)
- Tier 3: Moderate (Limited access to non-critical systems)
- Tier 4: Low (No direct system access)

2. Assessment Components:

a) Technical capability evaluation

b) Security controls assessment

c) Financial stability analysis

d) Regulatory compliance verification

e) Business continuity/disaster recovery capabilities

f) Insurance coverage review

3. VENDOR SECURITY REQUIREMENTS

1. All Tier 1 and Tier 2 Third Parties must:

a) Maintain SOC 2 Type II certification

b) Implement ISO 27001-compliant security controls

c) Conduct annual penetration testing

d) Maintain incident response capabilities

e) Provide real-time security monitoring

f) Support API-level security integration

2. Documentation Requirements:

a) Security policies and procedures

b) Compliance certificates

c) Insurance certificates

d) Incident response plans

e) Business continuity plans

f) Data handling procedures

4. MONITORING AND REVIEW PROCEDURES

1. Continuous Monitoring:

- Real-time security event monitoring
- Quarterly performance reviews
- Annual comprehensive assessments
- Incident reporting and tracking
- SLA compliance monitoring

2. Review Frequency:

- Tier 1: Quarterly
- Tier 2: Semi-annually
- Tier 3: Annually
- Tier 4: Bi-annually

5. CONTRACTUAL REQUIREMENTS

1. All Third-Party agreements must include:

a) Security requirements and standards

b) Data protection obligations

c) Audit rights

d) Incident reporting requirements

e) Service level agreements

f) Termination provisions

g) Insurance requirements

2. Minimum Insurance Requirements:

- Cyber liability: $10,000,000
- Professional liability: $5,000,000
- General liability: $2,000,000
- Workers' compensation: As required by law

6. INCIDENT MANAGEMENT AND REPORTING

1. Third Parties must report security incidents within:

- Critical incidents: 1 hour
- High severity: 4 hours
- Medium severity: 24 hours
- Low severity: 48 hours

2. Incident Response Requirements:

a) Initial notification

b) Detailed incident report

c) Root cause analysis

d) Remediation plan

e) Post-incident review

7. COMPLIANCE AND ENFORCEMENT

1. Compliance Monitoring:

- Regular compliance assessments

- Documentation reviews
- Security control testing
- Performance metrics tracking

2. Enforcement Actions:

a) Remediation requirements

b) Increased monitoring

c) Contract penalties

d) Service suspension

e) Contract termination

8. DOCUMENT CONTROL

1. Review and Updates:

- Annual review required
- Ad-hoc updates as needed
- Change control process
- Version tracking

2. Distribution Control:

- Confidential document
- Distribution limited to authorized personnel
- Version control maintained
- Electronic copies protected

APPROVAL AND EXECUTION

This Documentation is approved and adopted by DeepShield Systems, Inc. as of the date first written above.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Robert Kessler

Title: Chief Financial Officer

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

REVISION HISTORY

Version 1.0: January 11, 2024 - Initial documentation

Version 1.1: Pending review