SECURITY VENDOR MANAGEMENT PROTOCOL

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Security Vendor Management Protocol ("Protocol") establishes the requirements and procedures for evaluating, onboarding, and monitoring third-party vendors who may access, process, store, or transmit DeepShield Systems, Inc.'s ("Company") sensitive data, industrial control systems (ICS), or operational technology (OT) environments.

2. This Protocol applies to all vendors, contractors, and service providers who:

a) Have physical or logical access to Company systems or facilities

b) Process or store Company intellectual property or customer data

c) Provide components or services integrated into Company's security solutions

d) Support critical infrastructure protection services

2. DEFINITIONS

1. "Critical Vendor" means any third party whose services or products are essential to Company's core operations or whose failure could materially impact Company's ability to deliver services to customers.

2. "Security Assessment" means the systematic evaluation of a vendor's security controls, policies, and procedures according to Company's established criteria.

3. "Vendor Risk Rating" means the classification assigned to vendors based on their access level, criticality, and potential impact on Company operations.

3. VENDOR CLASSIFICATION AND RISK ASSESSMENT

1. All vendors shall be classified into one of the following tiers:

- Tier 1: Critical Infrastructure Vendors
- Tier 2: Core Technology Vendors

- Tier 3: Operational Support Vendors
- Tier 4: Administrative Vendors

2. Risk Assessment Requirements:

a) All Tier 1 and 2 vendors must undergo quarterly security assessments

b) Tier 3 vendors require annual assessments

c) Tier 4 vendors require biennial assessments

4. VENDOR ONBOARDING REQUIREMENTS

1. Pre-Engagement Due Diligence:

a) Security questionnaire completion

b) SOC 2 Type II report review (where applicable)

c) Penetration testing results review

d) Business continuity plan evaluation

e) Insurance coverage verification

2. Contractual Requirements:

a) Standard security addendum incorporation

b) Data protection agreements

c) Incident response obligations

d) Right-to-audit provisions

e) Breach notification requirements

5. ONGOING MONITORING AND COMPLIANCE

1. Continuous Monitoring Program:

a) Automated security scanning

b) Quarterly performance reviews

c) Annual compliance attestations

d) Security incident tracking

e) Service level agreement monitoring

2. Documentation Requirements:

a) Current security certifications

b) Updated insurance certificates

c) Annual security training records

d) Incident response test results

e) Vulnerability assessment reports

6. INCIDENT RESPONSE AND BREACH NOTIFICATION

1. Vendors must notify Company within:

a) 1 hour for critical security incidents

b) 4 hours for major security incidents

c) 24 hours for minor security incidents

2. Incident Response Requirements:

a) Initial incident report

b) Root cause analysis

c) Remediation plan

d) Post-incident review

e) Preventive measures implementation

7. TERMINATION AND OFFBOARDING

1. Vendor termination procedures must include:

a) Access revocation

b) Data return or destruction

c) Equipment recovery

d) Documentation archival

e) Final security assessment

2. Post-Termination Requirements:

a) Confidentiality obligations survive termination

b) Continuing security obligations

c) Post-termination audit rights

8. COMPLIANCE AND ENFORCEMENT

1. The Chief Security Officer shall be responsible for:

a) Protocol implementation oversight

b) Compliance monitoring

c) Exception management

d) Protocol updates

2. Non-compliance may result in:

a) Immediate vendor suspension

b) Contract termination

c) Legal remedies pursuit

9. PROTOCOL MAINTENANCE

1. This Protocol shall be reviewed and updated annually or upon:

a) Significant organizational changes

b) Regulatory requirement changes

c) Major security incidents

d) Risk assessment findings

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Protocol is executed by the authorized representatives of DeepShield Systems, Inc.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 15, 2024

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024