VENDOR SECURITY ASSESSMENT FRAMEWORK

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Vendor Security Assessment Framework ("Framework") establishes the security assessment requirements and procedures for all third-party vendors, contractors, and service providers (collectively "Vendors") that access, process, store, or transmit DeepShield Systems, Inc.'s ("DeepShield") data, systems, or networks, particularly those related to industrial control systems (ICS) and operational technology (OT) environments.

2. This Framework applies to all Vendors who:

a) Have access to DeepShield's proprietary technology or customer data

b) Provide components or services integrated into DeepShield's security platform

c) Support critical infrastructure protection solutions

d) Maintain or operate systems connected to DeepShield's network

2. DEFINITIONS

1. "Critical Systems" means any systems, networks, or infrastructure components that directly support DeepShield's core security platform or customer operations.

2. "Security Controls" means the management, operational, and technical safeguards implemented to protect the confidentiality, integrity, and availability of systems and data.

3. "Risk Level" means the categorization of vendors based on their access to systems and data, assessed as Tier 1 (Critical), Tier 2 (High), or Tier 3 (Moderate).

3. ASSESSMENT REQUIREMENTS

1. Initial Assessment

a) All prospective Vendors must complete DeepShield's Security Assessment Questionnaire

b) Submit current SOC 2 Type II or equivalent third-party security attestations

c) Provide documentation of security certifications (ISO 27001, NIST, etc.)

d) Complete technical security testing for direct system integrations

2. Risk Categorization

a) Tier 1: Direct access to Critical Systems or customer data

b) Tier 2: Indirect access to production systems or sensitive data

c) Tier 3: Limited access to non-critical systems or public data

3. Minimum Security Requirements

a) Documented information security program

b) Encryption of data in transit and at rest

c) Multi-factor authentication for system access

d) Regular security awareness training

e) Incident response and breach notification procedures

f) Vulnerability management program

4. ASSESSMENT PROCEDURES

1. Assessment Frequency

- Tier 1 Vendors: Annual comprehensive assessment
- Tier 2 Vendors: Biennial assessment
- Tier 3 Vendors: Initial assessment with periodic reviews

2. Assessment Components

a) Documentation review

b) Technical testing

c) On-site assessments (for Tier 1 Vendors)

d) Continuous monitoring

e) Compliance verification

3. Remediation Requirements

a) Critical findings must be remediated within 30 days

b) High-risk findings within 60 days

c) Medium-risk findings within 90 days

5. ONGOING MONITORING

1. DeepShield reserves the right to:

a) Conduct periodic security reviews

b) Request updated security documentation

c) Perform vulnerability scans

d) Audit Vendor compliance

e) Require security improvements

2. Vendors must notify DeepShield within 24 hours of:

a) Security incidents affecting DeepShield data or systems

b) Material changes to security controls

c) Compliance violations

d) Data breaches

6. COMPLIANCE AND ENFORCEMENT

1. Non-compliance may result in:

a) Suspension of system access

b) Termination of vendor relationship

c) Legal remedies as specified in service agreements

d) Financial penalties where applicable

2. Annual Compliance Review

a) Documentation of all assessments

b) Tracking of remediation efforts

c) Reporting to executive management

d) Updates to risk registers

7. CONFIDENTIALITY

1. All assessment results, security documentation, and related communications shall be treated as Confidential Information under applicable non-disclosure agreements.

8. MODIFICATIONS

1. DeepShield reserves the right to modify this Framework at any time with 30 days' notice to affected Vendors.

9. AUTHORIZATION

This Framework is authorized and approved by:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _

Document Control Number: DSS-SEC-VSA-2024-001