THIRD-PARTY VENDOR SECURITY REQUIREMENTS

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 2.4

1. PURPOSE AND SCOPE

1. This document establishes mandatory security requirements for all third-party vendors, contractors, and service providers (collectively "Vendors") that access, process, store, or transmit DeepShield Systems, Inc. ("DeepShield") data or provide services related to DeepShield's industrial control system (ICS) security infrastructure.

2. These requirements apply to all Vendors who:

a) Have access to DeepShield's networks, systems, or data

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

c) Support critical infrastructure protection solutions

d) Maintain or service operational technology (OT) environments

2. DEFINITIONS

1. "Critical Systems" means any systems, networks, or infrastructure components essential to DeepShield's core security platform operations.

2. "Sensitive Data" includes but is not limited to:

a) Customer infrastructure configurations

b) Security architecture specifications

c) Threat detection algorithms

d) Proprietary deep-layer security protocols

e) Maritime defense system parameters

3. "Security Incident" means any actual or suspected unauthorized access, disclosure, or breach of DeepShield systems or data.

3. SECURITY CONTROLS AND REQUIREMENTS

1. Access Control

a) Implementation of role-based access control (RBAC)

b) Multi-factor authentication for all privileged access

c) Unique credentials for each individual accessing DeepShield systems

d) Quarterly access rights review and certification

e) Immediate access termination upon personnel changes

2. Network Security

a) Segmented network architecture

b) Encrypted communications using TLS 1.3 or higher

c) Regular vulnerability scanning and penetration testing

d) Network monitoring and intrusion detection

e) Secure VPN for remote access

3. Data Protection

a) Encryption of data at rest using AES-256

b) Secure data transfer protocols

c) Regular backup and recovery testing

d) Data classification and handling procedures

e) Secure data disposal methods

4. COMPLIANCE AND CERTIFICATION

1. Vendors must maintain and provide evidence of:

a) ISO 27001 certification

b) SOC 2 Type II attestation

c) Industry-specific security certifications

d) Compliance with IEC 62443 standards

e) Annual security assessments

2. Documentation Requirements

a) Security policies and procedures

b) Incident response plans

c) Business continuity plans

d) Employee security training records

e) Audit logs and reports

5. INCIDENT RESPONSE AND REPORTING

1. Vendors must:

a) Notify DeepShield within 2 hours of any Security Incident

b) Provide initial incident assessment within 4 hours

c) Submit detailed incident reports within 24 hours

d) Cooperate fully in incident investigations

e) Maintain incident response capability 24/7/365

2. Post-Incident Requirements

a) Root cause analysis

b) Corrective action plans

c) Prevention measures

d) Impact assessment

e) Documentation of lessons learned

6. AUDIT AND ASSESSMENT RIGHTS

1. DeepShield reserves the right to:

a) Conduct security audits with 48 hours notice

b) Request security documentation at any time

c) Perform vulnerability assessments

d) Review security controls and configurations

e) Interview vendor security personnel

7. TERMINATION AND REMEDIATION

1. DeepShield may terminate vendor relationships for:

a) Material security violations

b) Failure to meet security requirements

c) Repeated security incidents

d) Non-compliance with audit requirements

e) Breach of confidentiality obligations

8. AMENDMENTS AND UPDATES

1. DeepShield may modify these requirements with 30 days notice to address:

a) New security threats

b) Regulatory changes

c) Technology evolution

d) Risk landscape changes

e) Operational requirements

9. ACKNOWLEDGMENT

The undersigned Vendor acknowledges receipt and acceptance of these security requirements:

Vendor Name: _

Authorized Representative: _

Title: _

Date: _

DeepShield Systems, Inc.

By: _

Title: _

Date: _