CLIENT DATA PROTECTION AGREEMENT

THIS CLIENT DATA PROTECTION AGREEMENT (the "Agreement") is made effective as of [DATE] by and between:

DEEPSHIELD SYSTEMS, INC., a Delaware corporation with its principal place of business at [ADDRESS] ("DeepShield" or the "Company")

and

[CLIENT NAME], a [JURISDICTION] [entity type] with its principal place of business at [ADDRESS] (the "Client")

(each a "Party" and collectively the "Parties")

1. RECITALS

WHEREAS, DeepShield provides industrial cybersecurity and critical infrastructure protection services, including operational technology (OT) security solutions, network monitoring, and threat detection services;

WHEREAS, in the course of providing such services, DeepShield may receive, process, store, or otherwise handle Client Data (as defined below);

WHEREAS, the Parties wish to establish terms and conditions governing the protection, security, and handling of Client Data;

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties agree as follows:

2. DEFINITIONS

1 "Client Data" means any data, information, or materials provided by or on behalf of Client to DeepShield, including but not limited to:

(a) Industrial control system (ICS) configurations and parameters

(b) SCADA network architecture and topology

(c) Operational technology specifications and protocols

(d) Security incident logs and alerts

(e) System performance metrics and operational data

(f) Client confidential information and trade secrets

2 "Security Standards" means industry-standard security measures, including ISO 27001, IEC 62443, and NIST Cybersecurity Framework controls.

3. DATA PROTECTION OBLIGATIONS

1 DeepShield shall:

(a) Implement and maintain appropriate technical and organizational measures to protect Client Data

(b) Process Client Data only as necessary to provide contracted services

(c) Restrict access to Client Data to authorized personnel with a need-to-know

(d) Maintain detailed access logs for all Client Data interactions

(e) Encrypt Client Data during transmission and at rest using industry-standard protocols

(f) Perform regular security assessments and penetration testing

2 DeepShield shall not:

(a) Use Client Data for any purpose other than providing contracted services

(b) Disclose Client Data to third parties without Client's prior written consent

(c) Transfer Client Data outside approved jurisdictions

(d) Retain Client Data longer than necessary for service delivery

4. SECURITY INCIDENT RESPONSE

1 DeepShield shall:

(a) Notify Client within 24 hours of discovering any Security Incident

(b) Provide detailed incident reports including scope, impact, and remediation

(c) Cooperate with Client's incident investigation and response

(d) Implement necessary corrective measures to prevent recurrence

2 "Security Incident" means any unauthorized access, disclosure, or breach of Client Data.

5. COMPLIANCE AND AUDIT RIGHTS

1 DeepShield shall maintain compliance with:

(a) Applicable data protection laws and regulations

(b) Industry security standards and best practices

(c) Client's reasonable security requirements

2 Client shall have the right to:

(a) Audit DeepShield's compliance annually with 30 days' notice

(b) Request security assessment reports and certifications

(c) Review DeepShield's security policies and procedures

6. CONFIDENTIALITY

1 DeepShield shall:

(a) Treat all Client Data as Confidential Information

(b) Protect Client Data with at least the same degree of care as its own confidential information

(c) Require personnel to sign confidentiality agreements

(d) Return or destroy Client Data upon contract termination

7. SUBCONTRACTORS

1 DeepShield shall:

(a) Obtain Client's prior written approval for subcontractors

(b) Ensure subcontractors are bound by equivalent obligations

(c) Remain liable for subcontractor compliance

(d) Maintain current list of approved subcontractors

8. LIABILITY AND INDEMNIFICATION

1 DeepShield shall indemnify Client for:

(a) Breaches of this Agreement

(b) Security Incidents caused by negligence

(c) Regulatory fines resulting from non-compliance

(d) Third-party claims arising from data breaches

9. TERM AND TERMINATION

1 This Agreement shall:

(a) Commence on the effective date

(b) Continue until termination of related service agreements

(c) Survive termination regarding existing Client Data

(d) Be terminable for material breach with 30 days' notice

10. GENERAL PROVISIONS

1 This Agreement shall be governed by Delaware law.

2 Amendments must be in writing and signed by both Parties.

3 If any provision is invalid, the remainder shall continue in effect.

4 This Agreement constitutes the entire agreement regarding Client Data protection.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first above written.

DEEPSHIELD SYSTEMS, INC.

By:

Name:

Title:

Date:

[CLIENT NAME]

By:

Name:

Title:

Date: