# INFRASTRUCTURE PROTECTION SERVICE LEVEL AGREEMENT

THIS INFRASTRUCTURE PROTECTION SERVICE LEVEL AGREEMENT (the "Agreement") is made effective as of [DATE] (the "Effective Date"), by and between:

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

and

[CLIENT NAME], a [STATE] corporation with its principal place of business at [ADDRESS] ("Client")

## 1. DEFINITIONS

1. "Critical Infrastructure Systems" means the Client's operational technology (OT) environments, industrial control systems (ICS), SCADA networks, and related industrial automation systems.

2. "Services" means the infrastructure protection services provided by Provider, including but not limited to continuous monitoring, threat detection, incident response, and system optimization.

3. "Service Levels" means the performance metrics and standards defined in Section 3 of this Agreement.

4. "Security Event" means any detected or suspected security incident, breach, or unauthorized access attempt affecting the Critical Infrastructure Systems.

## 2. SCOPE OF SERVICES

1. Provider shall deliver the following infrastructure protection services:

a) Real-time monitoring of Critical Infrastructure Systems

b) AI-driven threat detection and analysis

c) Automated incident response and mitigation

d) System performance optimization

e) Security compliance monitoring and reporting

f) 24/7 technical support

2. Geographic Coverage: Services shall be provided for Client's facilities located at [LOCATIONS].

3. System Integration: Provider shall maintain integration with Client's existing security infrastructure and operational technology environments.

## 3. SERVICE LEVELS

1. System Availability

a) Provider guarantees 99.99% uptime for monitoring and detection systems

b) Planned maintenance windows shall not exceed 4 hours per quarter

c) Emergency maintenance shall be communicated with minimum 2-hour notice

2. Incident Response Times

Critical (P1): 15 minutes

High (P2): 30 minutes

Medium (P3): 2 hours

Low (P4): 24 hours

3. Performance Metrics

a) False positive rate shall not exceed 0.1%

b) Threat detection accuracy shall maintain minimum 99.9%

c) System latency shall not exceed 100 milliseconds

## 4. REPORTING AND COMMUNICATIONS

1. Regular Reports

Provider shall deliver the following reports:

- Daily security status summaries
- Weekly performance metrics
- Monthly trend analysis
- Quarterly system health assessments

2. Incident Reporting

Security Events shall be reported according to the following protocol:

a) Initial notification within specified response time

b) Preliminary assessment within 1 hour

c) Detailed incident report within 24 hours

d) Post-incident analysis within 5 business days

## 5. CLIENT RESPONSIBILITIES

1. Client shall:

a) Provide necessary access to Critical Infrastructure Systems

b) Maintain current system documentation

c) Designate primary and backup technical contacts

d) Promptly implement recommended security measures

e) Participate in quarterly review meetings

## 6. COMPENSATION AND PAYMENT

1. Service Fees

Base Monthly Fee: [AMOUNT]

Additional Service Fees: As specified in Exhibit A

2. Service Credits

Provider shall issue service credits for failure to meet Service Levels according to the schedule in Exhibit B.

## 7. CONFIDENTIALITY AND DATA PROTECTION

1. Provider shall maintain strict confidentiality of all Client data and system information.

2. Data handling shall comply with [RELEVANT STANDARDS/REGULATIONS].

3. Provider shall maintain ISO 27001 certification and SOC 2 Type II compliance.

## 8. TERM AND TERMINATION

1. Initial Term: 36 months from the Effective Date

2. Renewal: Automatic 12-month renewal unless terminated with 90 days' notice

3. Termination for Cause: Either party may terminate for material breach with 30 days' written notice and opportunity to cure

## 9. LIMITATION OF LIABILITY

1. Provider's aggregate liability shall not exceed the total fees paid in the 12 months preceding the claim.

2. Neither party shall be liable for indirect, consequential, or punitive damages.

## 10. INSURANCE

Provider shall maintain:

a) Cyber liability insurance: $10,000,000

b) Professional liability insurance: $5,000,000

c) General liability insurance: $2,000,000

## 11. GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by Delaware law. Exclusive jurisdiction in Delaware courts.

## 12. ENTIRE AGREEMENT

This Agreement, including Exhibits A and B, constitutes the entire agreement between the parties regarding the subject matter herein.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

DEEPSHIELD SYSTEMS, INC.

**By: _**

Name: Dr. Marcus Chen

Title: Chief Executive Officer

**Date: _**

[CLIENT NAME]

**By: _**

**Name: _**

**Title: _**

**Date: _**