SERVICE LEVEL AGREEMENT

TERMINAL SECURITY SERVICES AND MONITORING

THIS SERVICE LEVEL AGREEMENT (the "Agreement") is made effective as of January 15, 2024 (the "Effective Date"), by and between:

DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2100 Harbor Bay Parkway, Suite 400, Alameda, CA 94502 ("Provider")

and

Long Beach Container Terminal LLC, a California limited liability company with its principal place of business at 1171 Pier F Avenue, Long Beach, CA 90802 ("Customer")

1. DEFINITIONS

1 "Critical Security Event" means any detected or suspected security breach, unauthorized access attempt, or cyber threat that poses immediate risk to Terminal Operations.

2 "Security Monitoring Services" means the continuous surveillance, threat detection, and response services provided through Provider's OT-SecureWatch(TM) platform.

3 "Terminal Operations" means all operational technology systems, industrial control systems, and related infrastructure within Customer's container terminal facility.

4 "Response Time" means the period between initial detection of a security event and Provider's implementation of countermeasures.

2. SERVICES

1 Provider shall deliver the following security services:

a) 24/7 real-time monitoring of Terminal Operations

b) AI-powered threat detection and analysis

c) Automated incident response for predefined threat scenarios

d) Monthly security assessment reports

e) Quarterly penetration testing of OT systems

f) Emergency response team availability

2 Service Availability

Provider guarantees 99.99% uptime for monitoring services, calculated monthly, excluding scheduled maintenance windows.

3. SERVICE LEVELS

1 Response Time Requirements:

Critical Security Events: 5 minutes

High Priority Events: 15 minutes

Medium Priority Events: 1 hour

Low Priority Events: 4 hours

2 Monthly Performance Metrics:

a) False Positive Rate: < 0.1%

b) Threat Detection Rate: > 99.9%

c) System Availability: > 99.99%

d) Alert Processing Time: < 30 seconds

4. REPORTING AND COMMUNICATIONS

1 Provider shall deliver:

a) Real-time security alerts via designated channels

b) Daily security summary reports

c) Monthly performance reports

d) Quarterly executive briefings

e) Annual security posture assessment

2 Communication Protocols:

Provider shall maintain dedicated secure communication channels for different severity levels, including encrypted messaging, secure voice lines, and emergency broadcast capabilities.

5. COMPLIANCE AND STANDARDS

1 Provider shall maintain compliance with:

a) MTSA requirements

b) ISPS Code standards

c) CBP security guidelines

d) ISO 27001 certification

e) NIST Cybersecurity Framework

6. SERVICE CREDITS

1 Performance Failures:

a) Critical Response Time Breach: 10% monthly fee credit

b) System Availability Breach: 5% monthly fee credit

c) Repeated Failures: Up to 25% monthly fee credit

7. TERM AND TERMINATION

1 Initial Term: 36 months from Effective Date

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

3 Termination for Cause: Immediate upon material breach

8. CONFIDENTIALITY

1 All security event data, system configurations, and response protocols shall be treated as Confidential Information under the Master Services Agreement dated December 1, 2023.

9. LIMITATION OF LIABILITY

1 Provider's aggregate liability shall not exceed twelve (12) months of fees paid under this Agreement.

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

10. GOVERNING LAW

This Agreement shall be governed by the laws of the State of California.

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

DEEPSHIELD SYSTEMS, INC.

By:

Name: Robert Kessler

Title: Chief Financial Officer

Date: January 15, 2024

LONG BEACH CONTAINER TERMINAL LLC

By:

Name: _

Title:

Date: