AUCKLAND PORT SECURITY FRAMEWORK 2023

1. INTRODUCTION AND PARTIES

This Auckland Port Security Framework ("Framework") is entered into as of July 1, 2023 ("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 ("Service Provider")

AND

Ports of Auckland Limited, a New Zealand corporation with its principal place of business at Sunderland Street, Auckland 1010, New Zealand ("Port Authority")

2. RECITALS

WHEREAS, the Port Authority operates critical maritime infrastructure requiring advanced cybersecurity protection for its operational technology (OT) systems;

WHEREAS, the Service Provider specializes in industrial control system (ICS) security solutions and maritime infrastructure protection;

WHEREAS, the parties desire to establish a comprehensive security framework for the protection of the Port's digital and physical infrastructure;

NOW, THEREFORE, the parties agree as follows:

3. DEFINITIONS

1 "Critical Systems" means all operational technology systems, including but not limited to terminal operating systems, vessel traffic management systems, cargo handling equipment, and associated control networks.

2 "Security Events" means any detected or suspected security incidents, breaches, or anomalies affecting Port operations.

3 "Framework Period" means the initial term of three (3) years from the Effective Date, unless terminated earlier pursuant to Section 8.

4. SCOPE OF SERVICES

1 The Service Provider shall implement and maintain:

(a) Real-time monitoring of all Critical Systems

(b) AI-driven threat detection and response capabilities

(c) Maritime-specific security modules for subsea infrastructure

(d) Integration with existing Port Authority security systems

(e) 24/7 Security Operations Center (SOC) support

2 Geographic Coverage shall include:

- Main container terminal
- Multi-cargo wharves
- Channel marker systems
- Harbor control facilities
- Associated maritime infrastructure

5. SECURITY PROTOCOLS

1 Threat Detection and Response

The Service Provider shall:

(a) Deploy DeepShield Maritime Defense(TM) platform

(b) Maintain < 15-minute response time for Critical Events

(c) Provide automated threat containment

(d) Generate detailed incident reports within 4 hours

2 System Integration Requirements

(a) Integration with SCADA networks

(b) Compatible with Navis N4 TOS

(c) Interface with vessel tracking systems

(d) Support for legacy OT protocols

6. COMPLIANCE AND REPORTING

1 The Service Provider shall ensure compliance with:

- Maritime Transport and Offshore Facilities Security Act 2004
- New Zealand Protective Security Requirements (PSR)
- ISO 27001 Information Security Standards
- International Ship and Port Facility Security (ISPS) Code

2 Regular reporting shall include:

(a) Monthly security status reports

(b) Quarterly compliance assessments

(c) Annual security audits

(d) Real-time security dashboards

7. CONFIDENTIALITY AND DATA PROTECTION

1 All security-related information shall be treated as strictly confidential.

2 Data handling shall comply with:

- Privacy Act 2020 (NZ)
- General Data Protection Regulation (where applicable)
- Maritime Security Information Sharing Protocols

8. TERM AND TERMINATION

1 Initial Term: Three (3) years from Effective Date

2 Renewal: Automatic one-year renewals unless terminated with 90 days' notice

3 Termination for Cause: Immediate upon material breach

9. FEES AND PAYMENT

1 Annual Service Fee: NZD 2,750,000

2 Payment Terms: Quarterly in advance

3 Annual Increase: Lesser of 3% or CPI

10. EXECUTION

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

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date:

PORTS OF OAKLAND LIMITED

By:

Name: [Port Authority Signatory]

Title: Chief Executive Officer

Date: