DUBAI PORTS WORLD CYBERSECURITY FRAMEWORK

Framework Version 2.3.1

Document ID: DSS-DPW-CSF-2024-001

Effective Date: January 15, 2024

1. FRAMEWORK OVERVIEW

1. This Cybersecurity Framework ("Framework") is established between DeepShield Systems, Inc., a Delaware corporation ("Provider"), and Dubai Ports World ("DPW") for the implementation and maintenance of maritime cybersecurity infrastructure.

2. The Framework governs the deployment, operation, and maintenance of Provider's DeepShield Maritime(TM) platform across DPW's designated port facilities and marine terminals.

2. DEFINITIONS

1. "Critical Infrastructure Components" means all operational technology (OT) systems, industrial control systems (ICS), and SCADA networks essential to port operations.

2. "Security Events" means any detected or suspected cybersecurity incidents, anomalies, or breaches affecting DPW's operational infrastructure.

3. "Platform" means Provider's proprietary DeepShield Maritime(TM) cybersecurity solution, including all associated software, hardware, and monitoring systems.

3. SECURITY ARCHITECTURE REQUIREMENTS

1. Provider shall implement a multi-layered security architecture incorporating:

a) Real-time monitoring of all Critical Infrastructure Components

b) AI-driven threat detection and response capabilities

c) Maritime-specific intrusion prevention systems (IPS)

d) Segregated operational technology networks

e) Encrypted communication channels for all control systems

2. The security architecture must maintain compliance with:

a) IEC 62443 Industrial Network Security Standards

b) NIST Framework for Improving Critical Infrastructure Cybersecurity

c) IMO Guidelines on Maritime Cyber Risk Management

d) UAE Information Assurance Standards

4. OPERATIONAL REQUIREMENTS

1. Provider shall maintain 24/7/365 security operations center (SOC) coverage with:

a) Maximum 15-minute response time for Critical Security Events

b) Dedicated maritime cybersecurity specialists

c) Direct escalation protocols to DPW's security team

d) Quarterly penetration testing and vulnerability assessments

2. Platform must achieve minimum 99.99% uptime for core security functions.

5. INCIDENT RESPONSE AND REPORTING

1. Provider shall:

a) Notify DPW within 30 minutes of any Critical Security Event

b) Provide detailed incident reports within 24 hours

c) Maintain chain of custody for all security incident evidence

d) Support post-incident forensic analysis

2. Monthly security reports shall include:

a) Threat intelligence specific to maritime operations

b) System performance metrics

c) Vulnerability assessment results

d) Remediation recommendations

6. COMPLIANCE AND AUDIT

1. Provider shall maintain all certifications required for maritime cybersecurity operations, including:

a) ISO 27001:2013

b) ISO 28000:2007

c) UAE NESA compliance

d) IACS Cyber Resilience requirements

2. DPW reserves the right to conduct annual security audits with 30 days' notice.

7. CONFIDENTIALITY AND DATA PROTECTION

1. Provider shall implement data protection measures complying with:

a) UAE Federal Law No. 2 of 2019 on Cybercrimes

b) GDPR requirements where applicable

c) DPW's internal data classification policies

2. All operational data shall be stored within UAE territory unless explicitly authorized by DPW.

8. TERM AND TERMINATION

1. This Framework shall remain in effect for an initial term of five (5) years.

2. Either party may terminate with 180 days' written notice for material breach.

9. GOVERNING LAW

1. This Framework shall be governed by the laws of the Dubai International Financial Centre (DIFC).

2. Any disputes shall be resolved through arbitration under DIFC-LCIA Arbitration Rules.

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: January 15, 2024

DUBAI PORTS WORLD

By: _

Name: [Authorized Signatory]

Title: [Title]

Date: _