BARCELONA PORT AUTHORITY SECURITY PROTOCOL

EFFECTIVE DATE: March 1, 2024

DOCUMENT NUMBER: DSS-BPA-2024-031

VERSION: 1.2

CLASSIFICATION: CONFIDENTIAL

1. PARTIES

This Security Protocol (the "Protocol") is entered into between:

DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2100 Innovation Drive, Suite 400, Boston, MA 02210 ("DeepShield")

AND

Barcelona Port Authority, a public entity established under Spanish law, with registered offices at World Trade Center Barcelona, Moll de Barcelona, s/n, 08039 Barcelona, Spain ("Port Authority")

2. RECITALS

WHEREAS, DeepShield provides advanced industrial cybersecurity solutions for maritime infrastructure protection;

WHEREAS, the Port Authority seeks to implement comprehensive cybersecurity measures for its operational technology (OT) environment;

WHEREAS, the parties desire to establish protocols for the deployment and operation of DeepShield's maritime security platform within the Port of Barcelona's critical infrastructure;

NOW, THEREFORE, the parties agree as follows:

3. DEFINITIONS

1 "Critical Systems" means all operational technology systems, SCADA networks, and industrial control systems within the Port Authority's infrastructure.

2 "Security Platform" means DeepShield's proprietary DeepShield Maritime(TM) cybersecurity solution.

3 "Security Incident" means any detected or suspected unauthorized access, breach, or cyber attack affecting Critical Systems.

4 "Response Team" means the joint incident response team comprised of DeepShield and Port Authority personnel.

4. SCOPE OF IMPLEMENTATION

1 **Coverage Areas**

- Terminal operating systems
- Vessel traffic management systems
- Cargo handling automation
- Access control infrastructure
- Maritime communication networks
- Emergency response systems

2 **Deployment Phases**

Initial assessment and network mapping

Security platform installation

System integration and testing

Personnel training

Full operational deployment

5. SECURITY MEASURES

1 **Continuous Monitoring**

- 24/7 real-time threat detection
- AI-driven anomaly identification
- Network traffic analysis
- System behavior monitoring
- Asset inventory tracking

2 **Access Controls**

- Multi-factor authentication for all critical systems
- Role-based access management

- Privileged account monitoring
- Access logging and audit trails
- Remote access security protocols

3 **Incident Response**

- Automated threat containment
- Predefined response procedures
- Escalation protocols
- Forensic data collection
- Incident documentation requirements

6. OPERATIONAL REQUIREMENTS

1 DeepShield shall:

- Maintain 99.99% platform uptime
- Provide 24/7 technical support
- Update threat intelligence feeds hourly
- Conduct monthly security assessments
- Deploy patches within 24 hours of release

2 Port Authority shall:

- Designate security coordinators
- Maintain network infrastructure
- Report suspicious activities
- Facilitate system access
- Participate in security drills

7. COMPLIANCE AND REPORTING

1 **Regulatory Compliance**

- EU NIS Directive
- ISPS Code requirements
- Spanish national security regulations
- Maritime cybersecurity guidelines

- Data protection requirements

2 **Regular Reporting**

- Daily security status reports
- Weekly incident summaries
- Monthly performance metrics
- Quarterly compliance reviews
- Annual security assessments

8. CONFIDENTIALITY

1 All security-related information, including but not limited to system configurations, vulnerabilities, and incident details, shall be treated as strictly confidential.

2 Information sharing shall comply with need-to-know principles and applicable data protection regulations.

9. TERM AND TERMINATION

1 This Protocol shall remain in effect for five (5) years from the Effective Date.

2 Either party may terminate for material breach with 90 days' written notice.

10. SIGNATURES

IN WITNESS WHEREOF, the authorized representatives of the parties have executed this Protocol as of the Effective Date.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date:

BARCELONA PORT AUTHORITY

By:

Name: [Port Authority Signatory]

Title: [Title]

Date:

11. EXHIBITS

Exhibit A: System Architecture Diagram

Exhibit B: Response Procedures

Exhibit C: Compliance Requirements

Exhibit D: Contact Matrix

[End of Document]