CRITICAL INFRASTRUCTURE PROTECTION PLAN

UAE PORTS FACILITIES

DeepShield Systems, Inc.

Document No. CIP-UAE-2024-001

Version 1.2 | Effective Date: January 15, 2024

1. INTRODUCTION

1 This Critical Infrastructure Protection Plan ("Plan") is established by DeepShield Systems, Inc., a Delaware corporation ("DeepShield"), for implementation at designated port facilities in the United Arab Emirates ("Protected Facilities").

2 This Plan complies with UAE Federal Law No. 5 of 2021 on Cybersecurity, International Ship and Port Facility Security (ISPS) Code requirements, and applicable maritime security regulations.

2. DEFINITIONS

1 "Critical Systems" means operational technology (OT) systems, industrial control systems (ICS), SCADA networks, and associated infrastructure essential to port operations.

2 "Security Architecture" means DeepShield's proprietary deep-layer security framework incorporating AI-driven threat detection, real-time monitoring, and adaptive defense mechanisms.

3 "Incident" means any actual or suspected security breach, unauthorized access, or cyber threat affecting Protected Facilities.

3. SCOPE AND APPLICABILITY

1 This Plan applies to all Critical Systems within Protected Facilities, including:

a) Terminal operating systems

b) Vessel traffic management systems

c) Cargo handling equipment

d) Access control systems

e) Maritime communication networks

f) Utility management systems

2 Geographic Coverage:

- Jebel Ali Port
- Port Khalifa
- Port Zayed
- Associated terminals and facilities

4. SECURITY ARCHITECTURE IMPLEMENTATION

1 Network Segmentation

a) Implementation of DeepShield's proprietary OT network isolation protocol

b) Establishment of secure communication channels between operational zones

c) Creation of demilitarized zones (DMZ) for external connections

2 Monitoring and Detection

a) Deployment of AI-powered anomaly detection systems

b) Real-time traffic analysis and behavioral monitoring

c) Integration with port authority security operations centers (SOCs)

3 Access Control

a) Multi-factor authentication for all critical system access

b) Role-based access control (RBAC) implementation

c) Privileged access management protocols

5. INCIDENT RESPONSE PROCEDURES

1 Initial Response

a) Immediate threat containment measures

b) Activation of backup systems and failover protocols

c) Notification to designated response team members

2 Investigation and Analysis

a) Forensic data collection procedures

b) Root cause analysis protocols

c) Impact assessment methodology

3 Recovery and Restoration

a) System restoration priorities

b) Data recovery procedures

c) Operational continuity measures

6. COMPLIANCE AND REPORTING

1 Regular compliance assessments shall be conducted quarterly, including:

a) Security architecture effectiveness evaluation

b) Regulatory compliance verification

c) Policy adherence audits

2 Reporting Requirements

a) Monthly security status reports to port authorities

b) Quarterly compliance reports to regulatory bodies

c) Immediate incident reporting as required by UAE law

7. MAINTENANCE AND UPDATES

1 This Plan shall be reviewed and updated:

a) Annually at minimum

b) Following significant security incidents

c) Upon major system modifications

d) As required by regulatory changes

8. CONFIDENTIALITY

1 This Plan contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure, copying, or distribution is strictly prohibited.

9. EXECUTION AND APPROVAL

IN WITNESS WHEREOF, this Critical Infrastructure Protection Plan is executed by the authorized representatives of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 15, 2024

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024

APPROVED BY:

[UAE Ports Authority Representative]

Date:

10. APPENDICES

Appendix A: System Architecture Diagrams

Appendix B: Emergency Contact List

Appendix C: Incident Response Flowcharts

Appendix D: Compliance Checklist

[End of Document]