MEXICAN GULF PORT SECURITY FRAMEWORK

DeepShield Systems, Inc.

Document Reference: DSS-MGPSF-2023-001

Effective Date: January 1, 2024

1. INTRODUCTION

1 This Mexican Gulf Port Security Framework ("Framework") is established by DeepShield Systems, Inc., a Delaware corporation ("DeepShield"), to govern the implementation and operation of industrial control system (ICS) security solutions at maritime facilities along the Gulf of Mexico.

2 This Framework incorporates requirements from the International Ship and Port Facility Security (ISPS) Code, U.S. Maritime Transportation Security Act (MTSA), and Mexican Port Security Standards (NOM-087-SCT4).

2. DEFINITIONS

1 "Critical Infrastructure" means essential operational technology systems, including but not limited to cargo handling equipment, access control systems, terminal operating systems, and vessel traffic management systems.

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

3 "Port Facility" means any maritime terminal, cargo handling facility, or port infrastructure within the Mexican Gulf region where DeepShield's systems are deployed.

3. SCOPE AND APPLICABILITY

1 Geographic Scope: This Framework applies to all Port Facilities along the Mexican Gulf Coast from Matamoros to Progreso.

2 System Coverage: The Framework governs all DeepShield security implementations, including:

a) SCADA network protection

b) Terminal automation systems

c) Access control infrastructure

d) Maritime communication networks

e) Cargo tracking systems

4. SECURITY ARCHITECTURE REQUIREMENTS

1 Minimum Security Controls

1.1 Implementation of DeepShield's AI-driven threat detection system

1.2 Real-time monitoring of all OT network traffic

1.3 Automated incident response capabilities

1.4 Redundant backup systems with 99.99% availability

2 Network Segmentation

2.1 Physical separation of IT and OT networks

2.2 Implementation of DMZ architecture

2.3 Secure remote access protocols

2.4 VLAN segregation for critical systems

5. OPERATIONAL PROTOCOLS

1 Threat Detection and Response

1.1 Continuous monitoring of network anomalies

1.2 Automated threat classification

1.3 Incident response procedures

1.4 Escalation protocols

2 System Maintenance

2.1 Quarterly security assessments

2.2 Monthly patch management

2.3 Configuration change control

2.4 Backup verification procedures

6. COMPLIANCE AND REPORTING

1 Regulatory Compliance

1.1 Adherence to Mexican maritime security regulations

1.2 MTSA compliance documentation

1.3 ISPS Code conformity assessments

1.4 Annual compliance audits

2 Performance Reporting

2.1 Monthly security metrics

2.2 Incident response statistics

2.3 System availability reports

2.4 Threat intelligence summaries

7. LIABILITY AND INDEMNIFICATION

1 DeepShield shall maintain professional liability insurance with coverage of not less than US$10,000,000 per occurrence.

2 Nothing in this Framework shall limit DeepShield's liability for:

a) Death or personal injury caused by negligence

b) Fraud or fraudulent misrepresentation

c) Willful misconduct or gross negligence

8. CONFIDENTIALITY

1 All security architecture details, threat intelligence, and incident response procedures shall be treated as Confidential Information.

2 Distribution of Framework documentation shall be limited to authorized personnel with appropriate security clearance.

9. AMENDMENTS AND UPDATES

1 This Framework shall be reviewed annually and updated as necessary to reflect:

a) Changes in threat landscape

b) Technological advancements

c) Regulatory requirements

d) Operational needs

10. EXECUTION

IN WITNESS WHEREOF, this Framework is executed by the authorized representative of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 1, 2024

WITNESS:

By:

Name: Sarah Blackwood

Title: Chief Technology Officer

Date: January 1, 2024