SECURITY COMPLIANCE FRAMEWORK DESIGN

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

Document Classification: Confidential

1. INTRODUCTION

1 This Security Compliance Framework Design document ("Framework") establishes the comprehensive security architecture and compliance requirements for DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security solutions and critical infrastructure protection platforms.

2 This Framework is binding upon all Company operations, development activities, and product deployments related to the DeepShield(TM) integrated industrial cybersecurity platform and associated services.

2. DEFINITIONS

1 "Critical Systems" means any industrial control systems, SCADA networks, or operational technology environments protected by Company solutions.

2 "Security Architecture" means the Company's proprietary deep-layer security infrastructure and associated protective mechanisms.

3 "Compliance Standards" means applicable regulatory requirements including but not limited to NIST SP 800-82, IEC 62443, NERC CIP, and maritime cybersecurity frameworks.

3. SECURITY ARCHITECTURE REQUIREMENTS

1 Core Security Components

a) Multi-layer defense architecture incorporating minimum N+1 redundancy

b) Real-time threat detection and response capabilities

c) AI-driven anomaly detection system with <0.001% false positive rate

d) Encrypted command and control channels using AES-256 minimum

e) Segmented network architecture with dedicated security zones

2 Authentication and Access Control

a) Multi-factor authentication for all privileged access

b) Role-based access control (RBAC) with principle of least privilege

c) Biometric verification for critical system changes

d) Automated access revocation protocols

e) Continuous session monitoring and validation

4. COMPLIANCE REQUIREMENTS

1 Regulatory Compliance

a) NIST Cybersecurity Framework alignment

b) IEC 62443 security level 3 minimum certification

c) NERC CIP-002 through CIP-013 compliance

d) Maritime cybersecurity requirements per IMO MSC-FAL.1/Circ.3

e) Regional critical infrastructure protection standards

2 Industry Standards

a) ISO 27001:2022 certification maintenance

b) ISA/IEC 62443 series alignment

c) NIST SP 800-82 Rev 2 guidelines

d) API 1164 compliance for pipeline systems

e) Classification society cybersecurity requirements

5. IMPLEMENTATION AND MONITORING

1 Security Controls Implementation

a) Automated deployment of security patches and updates

b) Continuous vulnerability assessment and remediation

c) Real-time threat intelligence integration

d) Automated incident response protocols

e) Regular penetration testing and security assessments

2 Performance Monitoring

a) 24/7 Security Operations Center (SOC) monitoring

b) Real-time metrics and KPI tracking

c) Monthly compliance assessment reports

d) Quarterly security posture reviews

e) Annual third-party security audits

6. INCIDENT RESPONSE AND RECOVERY

1 Incident Management

a) Automated threat containment procedures

b) Incident classification and escalation protocols

c) Mandatory reporting requirements

d) Evidence preservation procedures

e) Post-incident analysis requirements

2 Business Continuity

a) Recovery Time Objective (RTO) of <4 hours

b) Recovery Point Objective (RPO) of <15 minutes

c) Failover and redundancy requirements

d) Emergency response procedures

e) Crisis communication protocols

7. MAINTENANCE AND REVIEW

1 This Framework shall be reviewed and updated annually or upon significant changes to:

a) Regulatory requirements

b) Industry standards

c) Threat landscape

d) Technology infrastructure

e) Business operations

2 All updates require approval from:

a) Chief Security Architect

b) Chief Technology Officer

c) VP of Engineering

d) Compliance Officer

e) Legal Department

8. LEGAL DISCLAIMERS

1 This Framework contains confidential and proprietary information of DeepShield Systems, Inc. and is protected under applicable intellectual property laws.

2 No part of this Framework may be reproduced, modified, or distributed without express written authorization from the Company.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 15th day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

Sarah Blackwood

Chief Technology Officer

By:

James Morrison

VP of Engineering