NORTH SEA OIL PLATFORM PROTECTION PLAN

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

1. INTRODUCTION AND SCOPE

1 This North Sea Oil Platform Protection Plan (the "Protection Plan") sets forth the comprehensive cybersecurity and operational technology protection framework implemented by DeepShield Systems, Inc. ("DeepShield") for offshore oil and gas installations in the North Sea region.

2 This Protection Plan applies to all critical infrastructure protection services provided by DeepShield to North Sea operators pursuant to applicable Master Services Agreements.

2. DEFINITIONS

1 "Critical Systems" means all operational technology (OT) systems, industrial control systems (ICS), supervisory control and data acquisition (SCADA) networks, and related infrastructure essential to platform 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 "Platform" means any offshore oil or gas installation, including fixed platforms, floating production systems, and subsea infrastructure in the North Sea region.

3. PROTECTION FRAMEWORK

1 System Architecture

- Implementation of segregated OT/IT networks with unidirectional security gateways
- Deployment of hardened industrial firewalls at all network boundaries
- Installation of DeepShield's proprietary AI-enabled monitoring sensors
- Implementation of encrypted communication channels for all remote access

2 Threat Detection

- Continuous real-time monitoring of all OT network traffic

- AI-powered anomaly detection with platform-specific behavioral baselines
- Automated correlation of security events across platform systems
- Integration with global threat intelligence feeds specific to energy sector

3 Response Protocols

- Automated incident response for predefined threat scenarios
- Staged containment procedures based on threat severity
- Failsafe mechanisms for critical control systems
- Coordinated response procedures with platform operators

4. COMPLIANCE AND STANDARDS

1 This Protection Plan adheres to:

- IEC 62443 Industrial Network and System Security standards
- Norwegian Oil and Gas Association Guidelines 110
- UK Offshore Operators Association security frameworks
- EU NIS Directive requirements for critical infrastructure

2 Regular compliance assessments shall be conducted quarterly, with findings reported to platform operators within 15 business days.

5. OPERATIONAL REQUIREMENTS

1 Monitoring and Maintenance

- 24/7 security operations center (SOC) monitoring
- Monthly system health checks and updates
- Quarterly penetration testing of critical systems
- Annual comprehensive security architecture review

2 Personnel Requirements

- Minimum two DeepShield certified engineers assigned per platform
- Mandatory security clearance for all personnel
- Annual specialized training certification
- Compliance with platform-specific safety protocols

6. INCIDENT MANAGEMENT

1 Classification of Incidents

- Level 1: Minor anomalies requiring monitoring
- Level 2: Confirmed security threats requiring immediate response
- Level 3: Critical incidents affecting platform operations
- Level 4: Catastrophic events requiring emergency procedures

2 Response Procedures

- Immediate notification of platform operator for Level 2+ incidents
- Implementation of predetermined containment measures
- Activation of backup systems as required
- Documentation and post-incident analysis

7. LIABILITY AND LIMITATIONS

1 DeepShield shall maintain professional liability insurance coverage of not less than $50,000,000 USD per occurrence.

2 Nothing in this Protection Plan shall be construed to limit DeepShield's obligations under existing service agreements or applicable law.

8. CONFIDENTIALITY

1 All technical specifications, security configurations, and incident data shall be treated as strictly confidential information.

2 Information sharing shall comply with established protocols and applicable data protection regulations.

9. AMENDMENTS AND UPDATES

1 This Protection Plan shall be reviewed and updated annually or as required by material changes in threat landscape or regulatory requirements.

2 Amendments shall be communicated to all relevant parties with 30 days' notice unless immediate implementation is required for security purposes.

EXECUTION

IN WITNESS WHEREOF, this Protection Plan has been executed by the duly authorized representative of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 15, 2024