REGULATORY COMPLIANCE DOCUMENTATION

DeepShield Systems, Inc.

Last Updated: December 31, 2023

1. OVERVIEW AND PURPOSE

This document outlines DeepShield Systems, Inc.'s ("Company") regulatory compliance framework and certifications pertaining to its industrial cybersecurity solutions and critical infrastructure protection services. This documentation serves as a comprehensive record of the Company's compliance with applicable federal, state, and international regulations.

2. REGULATORY FRAMEWORK

2.1 Primary Regulatory Bodies

- U.S. Department of Homeland Security (DHS)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Energy Regulatory Commission (FERC)
- National Institute of Standards and Technology (NIST)
- European Union Agency for Cybersecurity (ENISA)

2.2 Key Regulations and Standards

- NERC CIP Standards (Version 7)
- IEC 62443 Industrial Network and System Security
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)
- EU NIS Directive 2016/1148
- Maritime Transportation Security Act (MTSA)

3. COMPLIANCE CERTIFICATIONS

3.1 Current Certifications

- ISO/IEC 27001:2013 Information Security Management
- ISO/IEC 27032:2012 Cybersecurity Guidelines
- SOC 2 Type II (Security, Availability, and Confidentiality)
- CMMC Level 3 Certification

- IEC 62443-4-1 Security for Industrial Automation and Control Systems

3.2 Certification Details

Certificate Name | Issuing Body | Issue Date | Expiration Date

----------|----------|----------|----------

ISO 27001 | BSI Group | 03/15/2023 | 03/14/2026

SOC 2 Type II | Deloitte & Touche LLP | 06/30/2023 | 06/29/2024

CMMC Level 3 | CMMC-AB | 09/01/2023 | 08/31/2026

4. COMPLIANCE MONITORING AND REPORTING

4.1 Internal Compliance Program

The Company maintains a comprehensive internal compliance program overseen by the Chief Compliance Officer and reviewed quarterly by the Board of Directors' Compliance Committee. Key components include:

a) Regular compliance audits

b) Employee training programs

c) Incident reporting procedures

d) Documentation maintenance

e) Risk assessment protocols

4.2 Reporting Requirements

The Company submits regular compliance reports to:

- DHS Cybersecurity Division (Quarterly)
- CISA Industrial Control Systems Joint Working Group (Semi-annually)
- State of Delaware Department of Technology and Information (Annually)

5. PRODUCT COMPLIANCE

5.1 DeepShield Platform Compliance

The Company's primary software platform maintains compliance with:

- NIST SP 800-82 Rev. 2
- IEC 62443-3-3 Security Requirements
- NERC CIP-005-7, CIP-007-7, CIP-010-4

- API 1164 Pipeline SCADA Security

5.2 Maritime Module Compliance

Additional compliance for maritime-specific modules:

- IMO MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management
- BIMCO Guidelines on Cyber Security Onboard Ships (Version 4.0)

6. RISK MANAGEMENT AND MITIGATION

6.1 Risk Assessment Framework

The Company employs a comprehensive risk assessment framework aligned with:

- NIST SP 800-30 Rev. 1
- ISO 31000:2018
- FAIR Risk Analysis Framework

6.2 Mitigation Strategies

Documented mitigation strategies include:

a) Continuous monitoring protocols

b) Incident response procedures

c) Business continuity planning

d) Supply chain security measures

7. COMPLIANCE UPDATES AND MAINTENANCE

This documentation is reviewed and updated quarterly by the Legal and Compliance Department. All updates are logged in the Company's compliance management system and approved by:

- Chief Compliance Officer
- General Counsel
- Chief Security Architect
- VP of Engineering

8. ATTESTATION

The undersigned hereby certifies that this documentation accurately reflects DeepShield Systems, Inc.'s current regulatory compliance status as of the date indicated below.

```

By: /s/ Jennifer Martinez

Name: Jennifer Martinez

Title: Chief Compliance Officer

Date: December 31, 2023

Witnessed By: /s/ Michael Thompson

Name: Michael Thompson

Title: General Counsel

Date: December 31, 2023

```

9. DISCLAIMER

This documentation is confidential and proprietary to DeepShield Systems, Inc. It may not be reproduced, distributed, or disclosed without prior written authorization. While the Company strives to maintain accurate and current compliance documentation, regulatory requirements are subject to change, and this document should not be considered legal advice.