REGULATORY CHANGE MANAGEMENT PROCEDURE

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: DSS-REG-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Regulatory Change Management Procedure ("Procedure") establishes the framework for identifying, assessing, implementing, and monitoring regulatory changes affecting DeepShield Systems, Inc.'s ("Company") operations in industrial cybersecurity and critical infrastructure protection.

2. This Procedure applies to all regulatory requirements governing:

a) Industrial Control System (ICS) security solutions

b) Critical infrastructure protection standards

c) Operational Technology (OT) security compliance

d) Maritime and subsea infrastructure security regulations

e) Cross-border data protection requirements

f) Industry-specific cybersecurity standards

2. DEFINITIONS

1. "Regulatory Change" means any modification, addition, or removal of laws, regulations, standards, or industry requirements affecting the Company's operations.

2. "Impact Assessment" means the formal evaluation of a regulatory change's effect on the Company's products, services, operations, or compliance obligations.

3. "Implementation Plan" means the documented strategy for achieving compliance with new or modified regulatory requirements.

3. RESPONSIBILITIES

1. Chief Compliance Officer (CCO):

- Overall responsibility for regulatory compliance

- Final approval of implementation plans
- Quarterly reporting to Board of Directors

2. Regulatory Change Committee:

- Monthly review of regulatory developments
- Impact assessment coordination
- Implementation oversight
- Compliance verification

3. Business Unit Leaders:

- Implementation of regulatory changes within their domains
- Resource allocation for compliance activities
- Regular status reporting to CCO

4. REGULATORY MONITORING PROCESS

1. The Company shall maintain subscriptions to the following regulatory information sources:

- Industrial Control Systems Joint Advisory Council (ICS-JAC)
- Maritime Cybersecurity Information Sharing Network (MCISN)
- Critical Infrastructure Protection Advisory Board (CIPAB)
- Regional cybersecurity regulatory authorities

2. The Regulatory Change Committee shall conduct monthly reviews of:

- Proposed regulations and standards
- Industry guidance and best practices
- Enforcement actions and regulatory interpretations
- Technical compliance requirements

5. IMPACT ASSESSMENT PROCEDURES

1. Initial Screening:

- Relevance determination
- Preliminary impact evaluation
- Urgency classification

- Resource requirement estimation

2. Detailed Assessment:

- Technical compliance analysis
- Operational impact evaluation
- Cost-benefit analysis
- Implementation timeline development
- Risk assessment

6. IMPLEMENTATION REQUIREMENTS

1. Implementation Plans shall include:

- Specific compliance objectives
- Required system modifications
- Training requirements
- Documentation updates
- Testing protocols
- Validation procedures

2. Change Management Controls:

- Version control procedures
- Configuration management
- System security maintenance
- Operational continuity measures

7. DOCUMENTATION AND RECORD KEEPING

1. The Company shall maintain records of:

- Regulatory change assessments
- Implementation plans and approvals
- Compliance verification results
- Training completion records
- Audit findings and resolutions

2. Record Retention:

- All documentation shall be retained for minimum 7 years
- Electronic records shall be maintained in secure, redundant storage
- Access controls shall be implemented per Information Security Policy

8. COMPLIANCE VERIFICATION

1. Internal Audit Requirements:

- Quarterly compliance reviews
- Annual comprehensive audits
- Ad-hoc assessments as needed

2. External Validation:

- Annual third-party compliance audits
- Regulatory certification maintenance
- Independent security assessments

9. REPORTING AND ESCALATION

1. Regular Reporting:

- Monthly status reports to Executive Committee
- Quarterly compliance dashboard to Board
- Annual regulatory compliance summary

2. Escalation Procedures:

- Immediate notification of critical compliance issues
- Rapid response protocols for regulatory inquiries
- Management notification thresholds

10. PROCEDURE MAINTENANCE

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

- Regulatory environment changes
- Organizational structure modifications
- Operational requirement updates

- Best practice evolution

2. All revisions require approval from:

- Chief Compliance Officer
- General Counsel
- Chief Executive Officer

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Marcus Chen

Chief Executive Officer

Date: January 15, 2024

By:

[Name]

Chief Compliance Officer

Date: January 15, 2024