CORPORATE LEGAL COMPLIANCE FRAMEWORK

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

1. INTRODUCTION AND PURPOSE

1. This Corporate Legal Compliance Framework (the "Framework") establishes the comprehensive compliance structure for DeepShield Systems, Inc. (the "Company"), a Delaware corporation specializing in industrial cybersecurity and critical infrastructure protection solutions.

2. This Framework is designed to ensure compliance with applicable federal, state, and international laws and regulations governing cybersecurity, critical infrastructure protection, and industrial control systems.

2. SCOPE AND APPLICABILITY

1. This Framework applies to all Company operations, subsidiaries, employees, contractors, and authorized representatives engaged in activities related to the Company's business.

2. Geographic Scope: Applies to all jurisdictions where the Company conducts business, with particular emphasis on:

a) United States federal and state regulations

b) Maritime jurisdiction compliance

c) International critical infrastructure standards

d) Cross-border data protection requirements

3. REGULATORY COMPLIANCE REQUIREMENTS

1. Cybersecurity Regulations

- NIST Cybersecurity Framework
- NERC CIP Standards
- Maritime Transportation Security Act (MTSA)
- EU NIS Directive
- Industrial Control Systems Security Requirements

2. Data Protection and Privacy

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- State-specific data protection laws
- Industry-specific privacy requirements

3. Export Control Compliance

- Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Sanctions and restricted party screening

4. COMPLIANCE GOVERNANCE STRUCTURE

1. Board Oversight

- Quarterly compliance reviews
- Annual compliance strategy approval
- Risk assessment evaluation

2. Management Responsibility

- Chief Compliance Officer appointment
- Departmental compliance liaisons
- Regular reporting requirements

3. Compliance Committee

- Composition: Legal, Security, Engineering, Operations
- Monthly meetings
- Incident response coordination

5. OPERATIONAL COMPLIANCE PROCEDURES

1. Product Development and Security

- Security-by-design principles
- Regulatory compliance verification
- Third-party component assessment

- Security testing protocols

2. Customer Engagement

- Due diligence requirements
- Contract compliance review
- Export control verification
- End-user certification

3. Supply Chain Management

- Vendor compliance assessment
- Security requirements for suppliers
- Continuous monitoring protocols

6. TRAINING AND AWARENESS

1. Required Training Programs

- Annual compliance certification
- Role-specific training modules
- Security awareness training
- Regulatory updates training

2. Documentation Requirements

- Training completion records
- Certification tracking
- Compliance attestations

7. AUDIT AND MONITORING

1. Internal Audit Program

- Quarterly compliance audits
- Technical security assessments
- Process verification reviews

2. External Audits

- Annual third-party compliance audit

- Certification maintenance requirements
- Regulatory examination preparation

8. INCIDENT RESPONSE AND REPORTING

1. Compliance Incident Response

- Incident classification matrix
- Reporting procedures
- Investigation protocols
- Remediation requirements

2. Regulatory Reporting

- Mandatory disclosure requirements
- Timeline compliance
- Documentation standards

9. ENFORCEMENT AND DISCIPLINARY ACTIONS

1. Compliance Violations

- Investigation procedures
- Progressive discipline framework
- Appeal process

2. Remediation Requirements

- Corrective action plans
- Monitoring periods
- Documentation requirements

10. FRAMEWORK MAINTENANCE AND UPDATES

1. Annual Review

- Framework assessment
- Regulatory update incorporation
- Best practice alignment

2. Version Control

- Change management procedures
- Distribution requirements
- Archive maintenance

AUTHORIZATION AND APPROVAL

This Framework has been reviewed and approved by the Board of Directors of DeepShield Systems, Inc.

APPROVED BY:

Dr. Marcus Chen

Chief Executive Officer

Date: January 15, 2024

Robert Kessler

Chief Financial Officer

Date: January 15, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024