EU NIS2 Directive Compliance Roadmap

DeepShield Systems, Inc.

Document Version: 1.0

Effective Date: January 15, 2024

1. Executive Summary

This document outlines DeepShield Systems, Inc.'s ("DeepShield") comprehensive strategy and implementation plan for achieving compliance with the EU Network and Information Systems 2 Directive (EU) 2022/2555 ("NIS2 Directive"). This roadmap addresses mandatory security requirements, incident reporting obligations, and risk management procedures as applicable to DeepShield's operations as a provider of cybersecurity solutions to essential entities and critical infrastructure operators.

2. Scope and Applicability

1. This roadmap applies to all DeepShield operations, products, and services provided within the European Union, particularly:

- Industrial Control System (ICS) security solutions
- SCADA network protection systems
- Maritime and subsea infrastructure security platforms
- Associated monitoring and incident response services

2. Territorial Scope:

- Direct operations in EU member states
- Services provided to EU-based essential entities
- Cross-border service provision affecting EU critical infrastructure

3. Compliance Requirements Assessment

1. Risk Management Measures

- Implementation of state-of-the-art technical security measures
- Regular security audits and vulnerability assessments
- Supply chain security verification procedures

- Encryption and access control protocols

2. Incident Reporting Obligations

- 24-hour initial notification requirements
- 72-hour detailed incident reporting procedures
- Establishment of dedicated incident response team
- Documentation and evidence preservation protocols

3. Business Continuity Requirements

- Development of business continuity plans
- Regular testing of backup and recovery procedures
- Crisis management protocols
- Service restoration priorities

4. Implementation Timeline

1. Phase 1: Initial Assessment and Planning (Q1 2024)

- Gap analysis completion
- Resource allocation
- Budget approval
- Stakeholder engagement

2. Phase 2: Technical Implementation (Q2-Q3 2024)

- Security control enhancement
- Monitoring system upgrades
- Documentation development
- Staff training initiation

3. Phase 3: Operational Integration (Q4 2024)

- Process implementation
- Testing and validation
- Compliance verification
- Final adjustments

5. Organizational Responsibilities

1. Executive Leadership

- Strategic oversight
- Resource allocation
- Final approval authority
- Compliance accountability

2. Technical Implementation Team

- Security architecture updates
- Control implementation
- Testing and validation
- Technical documentation

3. Legal and Compliance

- Regulatory interpretation
- Documentation review
- Reporting procedures
- Compliance monitoring

6. Risk Management Framework

1. Risk Assessment Procedures

- Quarterly risk assessments
- Threat modeling
- Vulnerability scanning
- Impact analysis

2. Control Implementation

- Technical controls
- Administrative controls
- Physical security measures
- Third-party risk management

7. Incident Response and Reporting

1. Incident Classification

- Severity levels
- Impact assessment
- Reporting thresholds
- Escalation criteria

2. Reporting Procedures

- Internal notification chain
- External reporting requirements
- Documentation requirements
- Follow-up protocols

8. Documentation and Record Keeping

1. Required Documentation

- Risk assessments
- Incident reports
- Audit trails
- Training records

2. Retention Requirements

- Document classification
- Retention periods
- Storage requirements
- Access controls

9. Budget and Resource Allocation

1. Implementation Budget

- Technical infrastructure: 750,000
- Training and certification: 200,000
- External consultants: 300,000
- Contingency: 250,000

2. Ongoing Compliance Costs

- Annual maintenance
- Regular audits
- Training updates
- Technology upgrades

10. Legal Disclaimer

This document is confidential and proprietary to DeepShield Systems, Inc. It contains sensitive information regarding security measures and compliance strategies. This roadmap is subject to revision based on regulatory updates, technical requirements, and operational needs. Nothing in this document constitutes legal advice or creates any contractual obligations.

11. Approval and Authorization

APPROVED AND ADOPTED by DeepShield Systems, Inc. on January 15, 2024.

_

Dr. Marcus Chen

Chief Executive Officer

_

Sarah Blackwood

Chief Technology Officer

_

Robert Kessler

Chief Financial Officer