CRITICAL INFRASTRUCTURE PROTECTION POLICY

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: DSS-CIP-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Critical Infrastructure Protection Policy ("Policy") establishes the framework and requirements for protecting critical infrastructure assets, operational technology (OT) environments, and industrial control systems (ICS) under DeepShield Systems, Inc.'s ("Company") purview or management.

2. This Policy applies to all Company employees, contractors, consultants, temporary workers, and other business partners who access, operate, maintain, or oversee critical infrastructure systems.

2. DEFINITIONS

1. "Critical Infrastructure" means systems, networks, and assets vital to national and economic security, public health, and safety.

2. "Operational Technology (OT)" refers to hardware and software that monitors and controls physical devices, processes, and events in industrial environments.

3. "Industrial Control Systems (ICS)" encompasses control systems and associated instrumentation used to operate and/or automate industrial processes.

3. INFRASTRUCTURE CLASSIFICATION

1. The Company shall maintain a comprehensive inventory of critical infrastructure assets categorized by:

a) Criticality Level (1-5)

b) Operational Impact

c) Security Requirements

d) Regulatory Compliance Obligations

2. Classification Review

- Annual review of asset classification
- Quarterly updates to asset inventory
- Immediate reclassification upon significant changes

4. SECURITY CONTROLS AND SAFEGUARDS

1. Physical Security

- Multi-layer access control systems
- 24/7 surveillance and monitoring
- Environmental controls and safeguards
- Backup power systems

2. Cybersecurity Measures

- Network segmentation and isolation
- Real-time threat monitoring
- Encrypted communications
- Access control and authentication
- Regular vulnerability assessments

3. Operational Controls

- Standard operating procedures
- Change management protocols
- Incident response procedures
- Business continuity planning

5. RISK ASSESSMENT AND MANAGEMENT

1. Regular Risk Assessments

- Quarterly vulnerability scanning
- Annual penetration testing
- Continuous monitoring and threat assessment
- Third-party security audits

2. Risk Mitigation

- Documented risk treatment plans
- Regular review and updates
- Executive oversight and approval

6. INCIDENT RESPONSE AND RECOVERY

1. Incident Response Team

- Defined roles and responsibilities
- 24/7 availability
- Regular training and exercises

2. Response Procedures

- Incident classification and escalation
- Communication protocols
- Documentation requirements
- Regulatory reporting obligations

7. COMPLIANCE AND AUDIT

1. Regulatory Compliance

- NERC CIP standards
- ISO 27001 requirements
- Industry-specific regulations
- Government mandates

2. Audit Program

- Internal audits (quarterly)
- External audits (annual)
- Compliance monitoring
- Documentation review

8. TRAINING AND AWARENESS

1. Required Training

- Initial orientation
- Annual refresher courses
- Role-specific training
- Incident response drills

2. Documentation

- Training records maintenance
- Certification tracking
- Competency assessments

9. POLICY REVIEW AND UPDATES

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

- Changes in technology
- New threats and vulnerabilities
- Regulatory requirements
- Organizational changes

2. All updates must be approved by the Chief Security Officer and Board of Directors.

10. ENFORCEMENT

1. Violations of this Policy may result in disciplinary action, up to and including termination of employment or business relationship.

2. The Company reserves the right to report violations to appropriate law enforcement authorities.

APPROVAL AND EXECUTION

This Policy is approved and adopted as of the Effective Date stated above.

FOR DEEPSHIELD SYSTEMS, INC.:

Dr. Marcus Chen

Chief Executive Officer

Dr. Elena Rodriguez

Chief Security Architect

Sarah Blackwood

Chief Technology Officer

[Document End]