NETWORK ARCHITECTURE SECURITY STANDARDS

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 3.2

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Network Architecture Security Standards document ("Standards") establishes mandatory security requirements and controls for all network infrastructure operated by DeepShield Systems, Inc. ("Company") in support of its industrial control system (ICS) security solutions and critical infrastructure protection services.

2. These Standards apply to all Company network environments, including:

a) Corporate IT networks

b) Development and testing environments

c) Customer-facing production systems

d) Operational Technology (OT) integration networks

e) Maritime and subsea infrastructure monitoring systems

2. NETWORK SEGMENTATION REQUIREMENTS

1. **Mandatory Network Zones**

The Company shall maintain strict separation between the following network zones:

- Zone 0: Internet-facing DMZ
- Zone 1: Corporate IT systems
- Zone 2: Development environments
- Zone 3: Customer production systems
- Zone 4: OT integration networks
- Zone 5: High-security enclaves

2. **Inter-Zone Communications**

All communication between zones must traverse security gateways implementing:

- Deep packet inspection

- Application-layer filtering
- Behavioral anomaly detection
- Real-time threat correlation
- Automated response capabilities

3. ACCESS CONTROL AND AUTHENTICATION

1. **Network Access Control**

All network access shall be governed by:

- Multi-factor authentication (MFA)
- Role-based access control (RBAC)
- Just-in-time access provisioning
- Automated access revocation
- Continuous session monitoring

2. **Privileged Access Management**

Administrative access to network infrastructure requires:

- Separate privileged access credentials
- Time-limited access tokens
- Video recording of sessions
- Real-time activity monitoring
- Secondary approval for critical changes

4. ENCRYPTION AND KEY MANAGEMENT

1. **Data in Transit**

All network traffic must be encrypted using:

- TLS 1.3 or higher for external communications
- IPSec with AES-256 for internal routing
- Quantum-resistant algorithms where available
- Perfect forward secrecy
- Certificate pinning

2. **Key Management**

Encryption key lifecycle shall be managed through:

- Hardware security modules (HSMs)
- Automated key rotation
- Split knowledge/dual control
- Secure key backup
- Regular key verification

5. MONITORING AND INCIDENT RESPONSE

1. **Network Monitoring**

Continuous monitoring shall include:

- Real-time traffic analysis
- Behavioral baseline enforcement
- Anomaly detection
- Asset inventory tracking
- Performance metrics

2. **Security Incident Response**

Network security incidents shall trigger:

- Automated containment measures
- Incident classification
- Response team notification
- Evidence preservation
- Customer impact assessment

6. COMPLIANCE AND AUDIT

1. **Compliance Requirements**

Network architecture must maintain compliance with:

- ISO 27001/27002
- IEC 62443
- NIST SP 800-82
- Maritime cybersecurity regulations

- Customer-specific requirements

2. **Audit Procedures**

Regular audits shall verify:

- Configuration compliance
- Security control effectiveness
- Policy enforcement
- Risk mitigation
- Documentation accuracy

7. MAINTENANCE AND UPDATES

1. **Change Management**

Network changes require:

- Security impact assessment
- Test environment validation
- Rollback procedures
- Customer notification
- Documentation updates

2. **Patch Management**

Security patches shall be:

- Evaluated within 24 hours
- Tested within 72 hours
- Deployed within defined SLAs
- Verified post-deployment
- Documented in change logs

8. DOCUMENT CONTROL

1. This document shall be reviewed annually and updated as required.

2. The Chief Security Architect maintains authority over this document.

3. Distribution is limited to authorized personnel only.

9. APPROVAL AND EXECUTION

APPROVED AND ADOPTED by DeepShield Systems, Inc.

By:

Dr. Elena Rodriguez

Chief Security Architect

Date:

By:

Sarah Blackwood

Chief Technology Officer

Date:

10. LEGAL DISCLAIMER