Network Security Configuration Standards

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: Confidential

1. Purpose and Scope

1. This Network Security Configuration Standards document ("Standards") establishes mandatory security configuration requirements for all network infrastructure, industrial control systems (ICS), and operational technology (OT) environments operated by or on behalf of DeepShield Systems, Inc. ("Company").

2. These Standards apply to all Company employees, contractors, consultants, temporary workers, and other business partners who access Company networks or industrial control systems.

2. Definitions

1. "Critical Infrastructure" means systems and assets designated as essential to Company operations, including SCADA networks, industrial automation systems, and maritime control infrastructure.

2. "Security Configuration" means the implementation of hardware, software, and firmware settings that ensure the confidentiality, integrity, and availability of network resources and data.

3. "OT Environment" means operational technology systems used to monitor and control industrial processes, including programmable logic controllers (PLCs), distributed control systems (DCS), and related components.

3. Network Segmentation Requirements

1. Industrial Control System Networks

a) ICS networks must maintain complete logical separation from corporate IT networks

b) Minimum three-tier architecture implementation required:

- Level 1: Control Network
- Level 2: Process Network
- Level 3: Manufacturing Operations Network

c) Inter-level communication restricted to documented essential services only

2. Maritime and Subsea Infrastructure

a) Dedicated network segments for subsea control systems

b) Physical separation of vessel control networks from crew networks

c) Satellite communication systems isolated via dedicated DMZ

4. Access Control Standards

1. Authentication Requirements

a) Multi-factor authentication mandatory for all privileged access

b) Biometric verification required for critical system access

c) Password complexity requirements:

- Minimum 16 characters
- Include uppercase, lowercase, numbers, special characters
- Maximum 60-day validity
- No password reuse for 24 cycles

2. Authorization Controls

a) Role-based access control (RBAC) implementation required

b) Principle of least privilege enforcement

c) Quarterly access review and certification

5. Security Monitoring and Response

1. Network Monitoring

a) Continuous real-time monitoring of all network segments

b) AI-driven anomaly detection systems required

c) Full packet capture on critical network segments

d) Minimum 90-day retention of security logs

2. Incident Response

a) Automated response capabilities for identified threats

b) Maximum 15-minute response time for critical alerts

c) Incident handling procedures must align with NIST SP 800-61r2

6. Encryption Standards

1. Data in Transit

a) TLS 1.3 or higher required for all network communications

b) IPSec with AES-256 minimum for VPN connections

c) Quantum-resistant algorithms required for critical infrastructure

2. Data at Rest

a) AES-256 minimum encryption standard

b) Hardware Security Module (HSM) required for key storage

c) Annual encryption key rotation mandatory

7. Configuration Management

1. Change Control

a) All configuration changes require documented approval

b) Testing in isolated environment mandatory

c) Roll-back procedures required for all changes

2. Documentation Requirements

a) Current network topology diagrams maintained

b) Configuration standards documented for each device type

c) Quarterly review and update of documentation

8. Compliance and Audit

1. Internal Audit Requirements

a) Quarterly security configuration audits

b) Monthly vulnerability assessments

c) Annual penetration testing

2. External Compliance

a) Annual third-party security assessment

b) Certification maintenance requirements:

- ISO 27001
- IEC 62443
- NIST CSF

9. Enforcement

1. Compliance with these Standards is mandatory. Violations may result in disciplinary action up to and including termination of employment or service agreements.

2. Exceptions to these Standards must be approved in writing by the Chief Security Architect and documented in the security exception register.

10. Document Control

Last Revised: January 15, 2024

Next Review Date: January 15, 2025

Document Owner: Chief Security Architect

Classification: Confidential

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.