WIRELESS NETWORK SECURITY POLICY

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: POL-SEC-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Wireless Network Security Policy ("Policy") establishes the standards, procedures, and requirements for wireless network access and security across DeepShield Systems, Inc.'s ("Company") corporate and operational technology environments.

2. This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel ("Users") accessing the Company's wireless networks, including but not limited to corporate WiFi, industrial wireless protocols, and wireless sensor networks used in critical infrastructure protection solutions.

2. DEFINITIONS

1. "Corporate Wireless Network" refers to all IEEE 802.11 wireless networks operated by the Company for business operations.

2. "Industrial Wireless Network" refers to wireless networks used in operational technology (OT) environments, including ISA100.11a, WirelessHART, and proprietary protocols.

3. "Security Architecture" means the Company's Deep-Layer Security Framework(TM) and associated security controls.

3. WIRELESS NETWORK CONFIGURATION REQUIREMENTS

1. Corporate Wireless Networks shall:

a) Implement WPA3-Enterprise encryption at minimum

b) Utilize IEEE 802.1X authentication with RADIUS server integration

c) Maintain separate SSIDs for corporate, guest, and IoT devices

d) Enable MAC address filtering and rogue access point detection

e) Implement network segmentation between wireless and wired networks

2. Industrial Wireless Networks shall:

a) Employ proprietary DeepShield encryption protocols

b) Implement frequency hopping spread spectrum (FHSS) technology

c) Maintain air-gapped separation from corporate networks

d) Enable intrusion detection specific to industrial protocols

e) Implement redundant communication paths

4. ACCESS CONTROL AND AUTHENTICATION

1. User Authentication Requirements:

a) Multi-factor authentication for all wireless network access

b) Integration with corporate identity management system

c) Unique credentials for each User

d) Automatic session termination after 30 minutes of inactivity

e) Password complexity requirements per Company standards

2. Device Authentication Requirements:

a) Certificate-based authentication for all devices

b) Automated device posture assessment

c) Compliance with Company's endpoint security standards

d) Regular security patch verification

e) Device registration in asset management system

5. MONITORING AND INCIDENT RESPONSE

1. The Company shall maintain continuous monitoring of wireless networks through:

a) Real-time traffic analysis

b) Wireless intrusion detection systems (WIDS)

c) RF spectrum analysis

d) Behavioral anomaly detection

e) Integration with Security Operations Center (SOC)

2. Incident Response Procedures:

a) Immediate isolation of affected network segments

b) Automated threat containment

c) Forensic data collection

d) Incident reporting per Company procedures

e) Post-incident analysis and remediation

6. COMPLIANCE AND AUDIT

1. Regular wireless security assessments shall be conducted, including:

a) Quarterly vulnerability scanning

b) Annual penetration testing

c) RF site surveys

d) Configuration compliance audits

e) Third-party security assessments

2. Documentation Requirements:

a) Maintenance of wireless network topology maps

b) Access control lists and authorization records

c) Security incident reports

d) Audit logs retention for minimum 1 year

e) Compliance verification records

7. POLICY ENFORCEMENT

1. Violations of this Policy may result in:

a) Immediate network access suspension

b) Disciplinary action up to termination

c) Legal action where applicable

d) Reporting to relevant authorities

e) Financial responsibility for damages

8. POLICY REVIEW AND UPDATES

1. This Policy shall be reviewed annually by the Information Security Committee.

2. Updates require approval from:

a) Chief Security Architect

b) Chief Technology Officer

c) Chief Information Security Officer

d) Legal Department

e) Executive Management

9. APPROVAL AND EXECUTION

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

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

Sarah Blackwood

Chief Technology Officer