Remote Access Security Policy

DeepShield Systems, Inc.

Version 3.0

Effective Date: January 15, 2024

1. Purpose and Scope

1. This Remote Access Security Policy ("Policy") establishes the requirements and procedures for secure remote access to DeepShield Systems, Inc.'s ("Company") network infrastructure, operational technology (OT) environments, and information systems.

2. This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel ("Users") who require remote access to Company systems, particularly those accessing industrial control systems (ICS), SCADA networks, and critical infrastructure protection platforms.

2. Definitions

1. "Remote Access" refers to any connection to Company networks or systems from an external location or non-Company managed network.

2. "Multi-Factor Authentication (MFA)" means authentication using at least two distinct factors: something you know (password), something you have (token), or something you are (biometric).

3. "Virtual Private Network (VPN)" refers to the Company's enterprise-grade encrypted network tunnel for secure remote connections.

3. Remote Access Authorization

1. All remote access must be explicitly authorized by:

a) The User's direct supervisor

b) Information Security Department

c) OT Security Team for industrial system access

2. Authorization requests must specify:

- Business justification
- Systems requiring access

- Duration of access requirement
- Level of access privileges needed

3. Authorizations shall be reviewed quarterly and automatically expire after 12 months unless renewed.

4. Technical Requirements

1. Mandatory Security Controls:

- Company-approved VPN client
- Multi-Factor Authentication
- Endpoint Detection and Response (EDR) software
- Current antivirus protection
- Host-based firewall
- Disk encryption
- Automatic screen lock after 10 minutes of inactivity

2. Device Requirements:

- Company-issued devices only for OT system access
- Current security patches and updates
- Compliance with Company's Device Security Standards
- Regular security posture assessments

3. Network Segmentation:

- Strict separation between IT and OT networks
- Role-based access controls
- Network traffic monitoring and logging
- Automated threat detection

5. Authentication and Access Control

1. All remote access connections must utilize:

- Unique user credentials
- Complex passwords meeting Company standards
- Hardware-based authentication tokens

- Session timeouts after 30 minutes of inactivity

2. Privileged Access Requirements:

- Just-in-time access provisioning
- Enhanced monitoring and logging
- Secondary approval for critical systems
- Time-limited access windows

6. Security Monitoring and Compliance

1. All remote access sessions shall be:

- Logged and monitored
- Subject to automated security analysis
- Recorded for audit purposes
- Reviewed for suspicious activity

2. Compliance Requirements:

- Quarterly compliance audits
- Annual security assessments
- Regular penetration testing
- Incident response drills

7. Incident Response and Reporting

1. Users must immediately report:

- Suspected security breaches
- Lost or stolen devices
- Compromised credentials
- Unusual system behavior

2. Security incidents will trigger:

- Immediate access suspension
- Security investigation
- Incident response procedures

- Regulatory notifications as required

8. Policy Enforcement

1. Violations of this Policy may result in:

- Immediate access termination
- Disciplinary action
- Legal proceedings
- Termination of employment or contract

9. Policy Review and Updates

1. This Policy shall be reviewed annually by the Information Security Committee and updated as necessary to maintain effectiveness and compliance with applicable regulations.

10. Document Control

Document Owner: Chief Security Architect

Last Review Date: January 15, 2024

Next Review Date: January 15, 2025

Version: 3.0

Classification: Confidential

Approval

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024