Endpoint Protection Implementation Guide

DeepShield Systems, Inc.

Document Version: 2.4

Effective Date: January 15, 2024

Classification: Confidential

1. Purpose and Scope

1. This Endpoint Protection Implementation Guide ("Guide") establishes mandatory security controls and implementation procedures for all endpoint devices connected to DeepShield Systems, Inc.'s ("Company") network infrastructure, including but not limited to workstations, servers, Industrial Control Systems (ICS), and Operational Technology (OT) devices.

2. This Guide applies to all Company employees, contractors, consultants, temporary workers, and other business partners accessing Company systems or handling Company data.

2. Definitions

1. "Endpoint" means any device that connects to the Company's network infrastructure, including but not limited to desktop computers, laptops, servers, industrial controllers, PLCs, RTUs, and smart devices.

2. "Critical Systems" refers to systems directly involved in the delivery of the Company's Industrial Cybersecurity Platform or supporting critical infrastructure protection services.

3. "Security Controls" means the technical, administrative, and physical safeguards implemented to protect Company assets.

3. Minimum Security Requirements

1. All Endpoints must implement:

a) Company-approved antivirus/anti-malware software with real-time protection

b) Host-based firewall configured to Company specifications

c) Disk encryption using AES-256 or stronger algorithms

d) Automated patch management system

e) Multi-factor authentication for system access

f) Logging and monitoring capabilities

2. Critical Systems must additionally implement:

a) Application whitelisting

b) Network segmentation

c) Enhanced logging and real-time monitoring

d) Specialized OT security protocols as defined in Schedule A

4. Implementation Procedures

1. Initial Configuration

a) System hardening per Company Baseline Security Standard

b) Removal of unnecessary services and applications

c) Implementation of least-privilege access controls

d) Configuration of security monitoring agents

2. Ongoing Maintenance

a) Weekly vulnerability scanning

b) Monthly security updates

c) Quarterly configuration reviews

d) Annual penetration testing

5. Compliance and Monitoring

1. The Company's Security Operations Center (SOC) shall:

a) Monitor endpoint compliance 24/7

b) Generate monthly compliance reports

c) Investigate and remediate security incidents

d) Maintain audit logs for minimum 365 days

2. Non-compliant endpoints shall be automatically quarantined until remediation is complete.

6. Incident Response

1. All security incidents must be reported to the SOC within one (1) hour of detection.

2. The incident response procedure shall follow the Company's Incident Response Plan (Document #SEC-IRP-2024).

7. Exceptions and Deviations

1. Exceptions to this Guide must be:

a) Documented using the Security Exception Request Form

b) Approved by the Chief Security Architect

c) Reviewed quarterly

d) Valid for maximum one (1) year

8. Review and Updates

1. This Guide shall be reviewed and updated:

a) Annually at minimum

b) Following major security incidents

c) Upon significant changes to Company infrastructure

d) As required by regulatory changes

9. Legal Compliance

1. This Guide is designed to ensure compliance with:

a) ISO 27001 requirements

b) NIST Cybersecurity Framework

c) Industry-specific regulations

d) Contractual obligations

10. Disclaimer

1. This Guide is confidential and proprietary to DeepShield Systems, Inc. Unauthorized disclosure, copying, or distribution is strictly prohibited.

2. The Company reserves the right to modify this Guide at any time without prior notice.

Approval and Authorization

APPROVED AND ADOPTED by the undersigned authorized representatives of DeepShield Systems, Inc.

Date: January 15, 2024

Dr. Elena Rodriguez

Chief Security Architect

Sarah Blackwood

Chief Technology Officer

[END OF DOCUMENT]