EDGE COMPUTING SECURITY IMPLEMENTATION GUIDE

DeepShield Systems, Inc.

Document Version: 1.2

Effective Date: January 15, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

1. This Edge Computing Security Implementation Guide ("Guide") establishes mandatory security controls and procedures for all edge computing deployments within DeepShield Systems, Inc.'s ("DeepShield") industrial control system (ICS) security infrastructure.

2. This Guide applies to all DeepShield employees, contractors, and authorized third parties involved in the implementation, maintenance, or operation of edge computing systems supporting DeepShield's proprietary deep-layer security architecture.

2. DEFINITIONS

1. "Edge Computing Environment" means any computational and storage resources deployed at or near the physical location where industrial control systems operate.

2. "Critical Security Parameters" or "CSPs" means security-related information (e.g., cryptographic keys, authentication data) whose disclosure or modification can compromise the security of edge computing implementations.

3. "Security Boundary" means the physical and logical perimeter within which edge computing security controls are implemented and enforced.

3. EDGE COMPUTING SECURITY ARCHITECTURE

1. Mandatory Security Controls

a) All edge computing nodes must implement DeepShield's proprietary Deep-Layer Security Protocol(TM) (DLSP) version 4.2 or higher.

b) Edge nodes shall maintain encrypted communication channels using AES-256 encryption with perfect forward secrecy.

c) Each edge computing deployment must maintain an isolated security domain with dedicated key management infrastructure.

2. Network Segmentation Requirements

a) Edge computing environments must implement physical and logical network separation from corporate IT networks.

b) VLAN segregation must be configured according to DeepShield's Network Segmentation Matrix (Doc. Ref: DS-NSM-2024).

4. IMPLEMENTATION PROCEDURES

1. Pre-deployment Security Assessment

a) Security architects must complete the Edge Computing Security Assessment Checklist (Form EC-SAC-01).

b) Risk assessment documentation must be approved by the Chief Security Architect or designee.

2. Hardware Security Requirements

a) All edge computing hardware must incorporate Trusted Platform Module (TPM) 2.0 or equivalent.

b) Physical security controls must comply with DeepShield's Physical Security Standard (Doc. Ref: DS-PSS-2024).

5. OPERATIONAL SECURITY CONTROLS

1. Access Control

a) Multi-factor authentication is mandatory for all administrative access.

b) Access privileges must be granted according to the Principle of Least Privilege.

c) Remote access must utilize DeepShield's Secure Remote Access Gateway (SRAG).

2. Monitoring and Incident Response

a) Continuous security monitoring must be implemented using DeepShield's AI-driven threat detection system.

b) Security events must be logged and retained according to the Security Event Logging Policy.

6. COMPLIANCE AND AUDIT

1. Internal Audit Requirements

a) Quarterly security audits of edge computing environments must be conducted.

b) Audit findings must be documented and remediated within timeframes specified in the Security Audit Policy.

2. Regulatory Compliance

a) Implementation must maintain compliance with applicable standards including NIST SP 800-82 and IEC 62443.

b) Documentation of compliance must be maintained and updated annually.

7. MAINTENANCE AND UPDATES

1. Security patches must be tested and deployed according to DeepShield's Patch Management Procedure.

2. Configuration changes must follow the Change Management Process and receive security review.

8. PROPRIETARY RIGHTS AND CONFIDENTIALITY

1. This Guide contains proprietary and confidential information of DeepShield Systems, Inc.

2. Unauthorized disclosure, reproduction, or use is strictly prohibited.

9. DOCUMENT CONTROL

Document Owner: Chief Security Architect

Review Cycle: Annual

Last Review Date: January 15, 2024

Next Review Date: January 15, 2025

APPROVAL

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: _

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _