

SECURITY IMPLEMENTATION WARRANTY

EFFECTIVE DATE: January 11, 2024

This Security Implementation Warranty (the "Warranty") is made and provided by DeepShield Systems, Inc., a Delaware corporation with its principal place of business at 2200 Innovation Drive, Suite 400, Wilmington, Delaware 19801 ("DeepShield" or the "Company").

1. DEFINITIONS

1. "Security Solutions" means the Company's proprietary industrial control system (ICS) security solutions, including but not limited to the DeepShield Platform(TM), OT Shield(TM), and Maritime Defense(TM) modules.
2. "Implementation Standards" means the security implementation protocols and procedures outlined in DeepShield's Security Implementation Framework version 4.2 or later.
3. "Critical Infrastructure Systems" means the industrial automation systems, SCADA networks, and operational technology environments protected by the Security Solutions.

2. WARRANTY SCOPE

1. DeepShield warrants that its Security Solutions, when properly implemented according to the Implementation Standards, will:
 - (a) Maintain continuous monitoring capabilities for protected Critical Infrastructure Systems;
 - (b) Detect and flag anomalous behavior patterns consistent with known threat signatures;
 - (c) Execute automated incident response protocols within 300 milliseconds of threat detection;
 - (d) Maintain 99.99% uptime for core security functions during normal operating conditions.
2. This Warranty applies exclusively to Security Solutions implemented by DeepShield-certified personnel or authorized implementation partners.

3. IMPLEMENTATION REQUIREMENTS

1. The Company warrants that all Security Solution implementations will:

- (a) Undergo pre-implementation security architecture review;
 - (b) Include comprehensive network topology mapping;
 - (c) Deploy redundant monitoring nodes at all critical junction points;
 - (d) Establish secure communication channels using AES-256 encryption;
 - (e) Configure automated backup and failover systems.
2. All implementations must pass DeepShield's 147-point security verification checklist before being deemed operational.

4. PERFORMANCE STANDARDS

1. The Security Solutions shall maintain:
- (a) Threat detection latency under 50 milliseconds;
 - (b) False positive rate below 0.01%;
 - (c) System resource utilization below 15% of host capacity;
 - (d) Real-time data processing capability of 100,000 events per second.
2. Performance metrics shall be continuously monitored and logged for warranty compliance verification.

5. WARRANTY PERIOD AND COVERAGE

1. This Warranty remains in effect for thirty-six (36) months from the date of implementation completion.
2. Coverage includes:
- (a) Security architecture remediation;
 - (b) Critical vulnerability patching;
 - (c) Threat detection engine updates;
 - (d) Implementation defect resolution.

6. EXCLUSIONS AND LIMITATIONS

1. This Warranty does not cover:

- (a) Unauthorized modifications to the Security Solutions;
- (b) Failures resulting from non-compliance with Implementation Standards;
- (c) Damage caused by force majeure events;
- (d) Integration with unauthorized third-party systems.

2. Maximum liability under this Warranty shall not exceed the original implementation cost.

7. REMEDIES

1. In the event of Warranty breach, DeepShield shall:

- (a) Investigate and remediate security implementation defects;
- (b) Provide necessary system upgrades or replacements;
- (c) Deploy emergency response teams if required;
- (d) Issue service credits per the Service Level Agreement.

8. COMPLIANCE AND CERTIFICATION

1. All Security Solution implementations are certified to comply with:

- (a) NIST Cybersecurity Framework;
- (b) IEC 62443 Industrial Security Standards;
- (c) Maritime Cybersecurity Framework (MCF) Guidelines;
- (d) Critical Infrastructure Protection (CIP) Standards.

9. GOVERNING LAW

1. This Warranty shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to conflicts of law principles.

10. EXECUTION

IN WITNESS WHEREOF, DeepShield Systems, Inc. has caused this Security Implementation Warranty to be executed by its duly authorized representative.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Marcus Chen

Title: Chief Executive Officer

Date: January 11, 2024