ISO 27001:2022 CERTIFICATION DOCUMENTATION

DeepShield Systems, Inc.

Document Reference: ISO-27001-2022-CERT-DS-2023

Effective Date: December 15, 2023

1. CERTIFICATION OVERVIEW

1. This document certifies that DeepShield Systems, Inc. ("DeepShield"), a Delaware corporation with principal offices at 2200 Innovation Drive, Suite 400, Wilmington, DE 19801, has successfully completed the ISO/IEC 27001:2022 certification audit and assessment process.

2. Certification Scope: The Information Security Management System (ISMS) covering the design, development, deployment, and support of DeepShield's industrial control system (ICS) security solutions, including:

- Deep-Layer Security Architecture Platform

- OT Network Monitoring Systems

- Maritime and Subsea Infrastructure Protection Modules

- SCADA Security Integration Services

- Industrial Automation Security Solutions

2. CERTIFICATION DETAILS

1. Certification Body:

- Name: Global Security Certifications International (GSCI)

- Accreditation Number: AB-27001-US-2145

- Lead Auditor: Dr. Jonathan Walsh, CISA, CISSP

- Certificate Number: DS-27001-2023-12-15-001

2. Certification Period:

- Issue Date: December 15, 2023

- Valid Until: December 14, 2026

- Surveillance Audits: Scheduled annually (December 2024, December 2025)

3. CERTIFIED LOCATIONS

1. Primary Development Center:

-       2200 Innovation Drive, Suite 400, Wilmington, DE 19801

2. Secondary Facilities:

-       Research & Development: 100 Technology Park, Boston, MA 02210

-       Security Operations Center: 555 Cyber Avenue, Austin, TX 78701

-       Customer Support Hub: 800 Maritime Plaza, Seattle, WA 98101

4. ISMS SCOPE STATEMENT

1. The certified Information Security Management System encompasses:

a) All information assets, systems, and processes related to DeepShield's industrial cybersecurity solutions

b) Development and maintenance of proprietary security algorithms

c) Customer data processing and storage systems

d) Cloud-based monitoring and response infrastructure

e) Internal corporate systems and networks

f) Physical security controls at all listed facilities

2. Exclusions: None

5. COMPLIANCE VERIFICATION

1. DeepShield has demonstrated compliance with all mandatory requirements of ISO/IEC 27001:2022, including:

a) Context of the organization (Clause 4)

b) Leadership and commitment (Clause 5)

c) Planning and risk assessment (Clause 6)

d) Support and resource allocation (Clause 7)

e) Operational controls and security measures (Clause 8)

f) Performance evaluation (Clause 9)

g) Continuous improvement (Clause 10)

2. Implementation of all applicable controls from ISO/IEC 27002:2022 has been verified through

comprehensive audit procedures.

6. STATEMENT OF APPLICABILITY

1. DeepShield maintains a detailed Statement of Applicability (Reference: SOA-27001-2023-V1) documenting the implementation status of all ISO 27001:2022 controls.

2. Critical control areas with verified implementation include:

- Information security policies
- Asset management
- Access control
- Cryptography
- Physical security
- Operations security
- Communications security
- System acquisition and development
- Supplier relationships
- Incident management
- Business continuity
- Compliance

7. CERTIFICATION MAINTENANCE

1. DeepShield commits to:

- Maintaining the ISMS in accordance with ISO 27001:2022 requirements
- Conducting internal audits at planned intervals
- Participating in surveillance audits by the certification body
- Implementing continuous improvement processes
- Promptly addressing any identified nonconformities

8. AUTHORIZATION

This certification documentation is hereby validated and authorized:

```

GLOBAL SECURITY CERTIFICATIONS INTERNATIONAL

**By:** _

Dr. Jonathan Walsh

Lead ISO 27001 Auditor

Certificate No: LA-27001-US-892

Date: December 15, 2023

```

```

DEEPSHIELD SYSTEMS, INC.

**By:** _

Dr. Elena Rodriguez

Chief Security Architect

Date: December 15, 2023

```

9. LEGAL NOTICES

1. This certification documentation is the property of DeepShield Systems, Inc. and may not be modified, transferred, or reproduced without written authorization.

2. The ISO 27001:2022 certification status is subject to ongoing compliance with standard requirements and successful completion of surveillance audits.

End of Document