DeepShield Systems ISO/IEC 27001:2022 Information Security Certification Report

Report Date: January 11, 2024

Certificate Number: ISO27001-2022-DS-7845

Organization: DeepShield Systems, Inc.

Scope Location: 2300 Cyber Drive, Suite 400, Wilmington, DE 19801

Certification Body: Global Security Certifications Ltd.

Lead Auditor: Dr. Thomas Richardson, CISA, CISSP

Audit Period: October 15, 2023 - December 20, 2023

1. Executive Summary

This report documents the successful certification of DeepShield Systems, Inc.'s Information Security Management System (ISMS) under ISO/IEC 27001:2022 standards. The certification scope encompasses all information security processes related to the development, deployment, and support of DeepShield's industrial control system (ICS) security solutions and critical infrastructure protection platforms.

2. Scope of Certification

2.1 Business Activities Covered

- Development and maintenance of industrial cybersecurity software solutions
- Cloud-based security monitoring and threat detection services
- Customer support and incident response operations
- Research and development of AI-driven security algorithms
- Maritime and subsea infrastructure protection systems

2.2 Locations

- Primary Development Center: Wilmington, DE
- Security Operations Center: Austin, TX
- R&D Laboratory: Boston, MA
- Data Centers: US-East-1, US-West-2

2.3 Technical Systems

- Development infrastructure
- Production environments
- Customer-facing platforms
- Internal corporate systems
- Cloud service infrastructure

3. Assessment Methodology

3.1 Audit Approach

The certification audit was conducted using a risk-based approach, examining DeepShield's ISMS against all mandatory requirements of ISO/IEC 27001:2022. The assessment included:

- Document review
- Process observation
- Personnel interviews
- Technical testing
- Control validation

3.2 Sampling Methodology

Statistical sampling was employed across all control domains, with emphasis on critical security processes. Sample size was determined using AQL Level II inspection criteria.

4. Findings and Observations

4.1 Strengths

Robust risk assessment framework specifically adapted for industrial environments

Advanced threat modeling incorporating OT-specific scenarios

Comprehensive incident response procedures with industrial sector focus

Strong integration between security controls and business objectives

Effective security awareness training program

4.2 Nonconformities

No major nonconformities were identified. Three minor nonconformities were documented:

Documentation update procedures (Clause 7.5.3) - Resolved

Asset management records (Annex A.8.1) - Resolved

Supplier security assessment (A.15.2) - Resolved

4.3 Opportunities for Improvement

Enhanced metrics for measuring security control effectiveness

Strengthened change management documentation

Extended security monitoring coverage for remote development teams

5. Control Implementation

5.1 Leadership and Planning

- Demonstrated executive commitment through security steering committee
- Clear security objectives aligned with business strategy
- Comprehensive risk management framework
- Regular management review process

5.2 Operation and Support

- Documented information security procedures
- Implemented security incident management system
- Established business continuity protocols
- Regular security testing and validation

5.3 Performance Evaluation

- Security metrics dashboard
- Internal audit program
- Continuous monitoring system
- Regular management review meetings

6. Certification Decision

Based on the comprehensive assessment of DeepShield Systems' ISMS, Global Security Certifications Ltd. has determined that the organization meets all requirements of ISO/IEC 27001:2022. The certification is granted with the following details:

- Initial Certification Date: January 11, 2024

- Certificate Expiry Date: January 10, 2027
- Surveillance Audits: January 2025, January 2026

7. Maintenance Requirements

To maintain certification, DeepShield Systems must:

Conduct annual internal audits

Participate in surveillance audits

Address any nonconformities within specified timeframes

Maintain documentation of all security incidents

Continue management review processes

8. Attestation

This certification report accurately reflects the results of the ISO/IEC 27001:2022 certification audit of DeepShield Systems, Inc.'s Information Security Management System.

```

_

Dr. Thomas Richardson, CISA, CISSP

Lead Auditor

Global Security Certifications Ltd.

Date: January 11, 2024

```

```

_

Margaret Wells

Certification Manager

Global Security Certifications Ltd.

Date: January 11, 2024

```

9. Confidentiality Statement

This report contains confidential information about DeepShield Systems, Inc.'s information security management system. Distribution is restricted to authorized personnel only. All recipients must maintain confidentiality and implement appropriate security controls to protect this information.