CYBER LIABILITY INSURANCE POLICY

Policy Number: CYB-2023-DS-8842

Named Insured: DeepShield Systems, Inc.

Policy Period: January 1, 2023 to January 1, 2024

Retroactive Date: March 15, 2016

Premium: $875,000

I. DECLARATIONS

A. COVERAGE LIMITS AND RETENTIONS

- Aggregate Policy Limit: $25,000,000
- Per Occurrence Limit: $10,000,000
- Business Interruption Coverage: $5,000,000
- Data Recovery Costs: $3,000,000
- Cyber Extortion Coverage: $5,000,000
- Retention (each claim): $250,000

B. TERRITORIAL LIMITS

Worldwide coverage, excluding sanctioned countries as defined by OFAC

II. INSURING AGREEMENTS

A. NETWORK SECURITY AND PRIVACY LIABILITY

Covers losses arising from:

Unauthorized access or use of computer systems

Transmission of malicious code

Denial of service attacks

Privacy breaches involving protected information

Failure to prevent unauthorized disclosure of client data

B. INDUSTRIAL CONTROL SYSTEM (ICS) PROTECTION

Specific coverage for:

SCADA system breaches

OT network compromises

Maritime control system failures

Subsea infrastructure protection failures

Manufacturing system interruptions

III. SPECIALIZED ENDORSEMENTS

A. CRITICAL INFRASTRUCTURE EXTENSION

Additional coverage for:

Industrial automation system failures

Control system ransomware events

Supply chain cyber incidents

Operational technology disruptions

B. MARITIME OPERATIONS COVERAGE

Specific protection for:

Vessel control system breaches

Port facility cyber incidents

Offshore platform security events

Subsea control system failures

IV. EXCLUSIONS

This policy does not cover:

Prior known incidents before policy inception

Intentional acts by insured

War and terrorism (except cyber terrorism)

Nuclear incidents

Property damage (except as specifically covered)

Bodily injury (except as specifically covered)

Infrastructure failure not directly caused by cyber event

Contractual liability outside covered services

V. CLAIMS CONDITIONS

A. NOTIFICATION REQUIREMENTS

Written notice within 72 hours of discovery

Immediate notification for ransomware events

Detailed incident documentation

Cooperation with forensic investigation

B. INCIDENT RESPONSE

Use of approved incident response vendors

Mandatory coordination with insurer's cyber response team

Implementation of required mitigation measures

Regular status updates to insurer

VI. POLICY CONDITIONS

A. MATERIAL CHANGES

Insured must notify within 30 days of:

Acquisition of new subsidiaries

Change in security controls

Material modification of covered systems

New high-risk client contracts

B. SECURITY REQUIREMENTS

Insured must maintain:

Updated incident response plan

Regular security assessments

Employee cybersecurity training

Patch management program

Backup and recovery procedures

VII. DEFINITIONS

A. "Computer System" means all electronic computers, software, data storage devices, and all components thereof.

B. "Industrial Control System" means hardware and software controls used to operate industrial processes.

C. "Critical Infrastructure" means systems and assets vital to national security, economic security, or public health and safety.

D. "Operational Technology" means hardware and software that monitors and controls physical devices and processes.

VIII. ENDORSEMENT SCHEDULE

Maritime Operations Extension (Form ME-2023)

Critical Infrastructure Protection (Form CIP-2023)

Regulatory Investigation Coverage (Form RIC-2023)

Social Engineering Coverage (Form SEC-2023)

IX. AUTHORIZATION

This policy is valid when signed by an authorized representative of the insurer and the named insured.

For the Insurer:

[Signature Line]

Name: _

Title: _

Date: _

For DeepShield Systems, Inc.:

[Signature Line]

Name: Robert Kessler

Title: Chief Financial Officer

Date: December 15, 2022