INCIDENT RESPONSE INSURANCE COVERAGE DOCUMENTATION

DeepShield Systems, Inc.

Effective Date: January 1, 2024

1. COVERAGE OVERVIEW

1 This document details the incident response insurance coverage maintained by DeepShield Systems, Inc. ("Company") for cyber incidents, operational technology disruptions, and related security events affecting industrial control systems and critical infrastructure protection services.

2 Primary Coverage Provider: CyberTech Insurance Corporation

Policy Number: CTI-2024-DS-785492

Coverage Period: January 1, 2024 - December 31, 2024

Aggregate Coverage Limit: $50,000,000

2. COVERED INCIDENTS

1 First-Party Coverage:

- Industrial control system breaches
- SCADA network compromises
- Operational technology disruptions
- Maritime infrastructure security incidents
- AI system malfunctions
- Deep-layer security architecture failures
- Real-time monitoring system outages
- Automated incident response system failures

2 Third-Party Coverage:

- Customer data breaches
- Service interruption claims
- Professional liability claims
- Technology errors and omissions

- Regulatory compliance violations
- Critical infrastructure downtime claims
- Manufacturing operations disruption claims

3. COVERAGE LIMITS AND SUBLIMITS

1 Primary Coverage Components:

- Incident Response Costs: $10,000,000 per occurrence
- Business Interruption: $15,000,000 per occurrence
- System Restoration: $8,000,000 per occurrence
- Cyber Extortion: $5,000,000 per occurrence
- Regulatory Defense: $7,000,000 per occurrence

2 Specialized Coverage Sublimits:

- Maritime Infrastructure Events: $12,000,000
- AI System Failures: $6,000,000
- Industrial Control System Recovery: $8,000,000
- SCADA Network Restoration: $7,000,000

4. INCIDENT RESPONSE PROCEDURES

1 Initial Notification Requirements:

- Immediate notification to insurer's incident response hotline
- Written notification within 24 hours of discovery
- Preliminary incident assessment within 48 hours
- Engagement of approved incident response vendors

2 Documentation Requirements:

- Detailed incident timeline
- System impact assessment
- Customer notification records
- Remediation action plan
- Cost documentation
- Third-party communications

- Regulatory reporting records

5. APPROVED INCIDENT RESPONSE VENDORS

1 Digital Forensics:

- CyberTrace Analytics, LLC
- Industrial Security Forensics Group
- Maritime Technology Investigation Services

2 Legal Services:

- Thompson & Bradley LLP
- Maritime Technology Law Group
- Critical Infrastructure Defense Counsel

3 Technical Recovery:

- Industrial Systems Recovery Team
- OT Network Specialists, Inc.
- Deep Architecture Restoration Services

6. EXCLUSIONS AND LIMITATIONS

1 General Exclusions:

- Prior known incidents
- Intentional acts by employees
- War and terrorism
- Nuclear incidents
- Environmental hazards

2 Specific Exclusions:

- Non-approved vendor costs
- Unproven technology implementations
- Experimental AI applications
- Non-compliant system configurations
- Unauthorized system modifications

7. CLAIMS PROCEDURES

1 Claims Submission Requirements:

- Initial notice within 72 hours
- Complete claim documentation within 30 days
- Supporting evidence preservation
- Cooperation with investigators
- Regular status updates

2 Claims Documentation:

- Incident response logs
- System restoration costs
- Business interruption calculations
- Third-party damage assessments
- Regulatory compliance records

8. POLICY MAINTENANCE

1 The Company shall maintain:

- Updated system inventory
- Current risk assessments
- Security compliance documentation
- Incident response plans
- Employee training records
- Vendor management procedures

9. AUTHORIZATION

This document accurately reflects the incident response insurance coverage maintained by DeepShield Systems, Inc. as of the effective date stated above.

APPROVED AND ACCEPTED:

_

Robert Kessler

Chief Financial Officer

DeepShield Systems, Inc.

Date: _

_

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _