CYBERSECURITY INCIDENT RESPONSE PLAN

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

1. PURPOSE AND SCOPE

1. This Cybersecurity Incident Response Plan ("Plan") establishes the procedures and responsibilities for responding to cybersecurity incidents affecting DeepShield Systems, Inc.'s ("Company") information systems, operational technology environments, and client infrastructure.

2. This Plan applies to all employees, contractors, and third-party service providers who have access to Company systems or client environments, including but not limited to industrial control systems (ICS), SCADA networks, and maritime security infrastructure.

2. DEFINITIONS

1. "Cybersecurity Incident" means any actual or suspected event that threatens the confidentiality, integrity, or availability of Company information systems, client infrastructure, or protected data.

2. "Critical Infrastructure" means systems, networks, and assets designated as essential to Company or client operations, including industrial control systems, maritime facilities, and offshore platforms.

3. "Incident Response Team" or "IRT" means the cross-functional team responsible for implementing this Plan, as detailed in Section 3.

3. INCIDENT RESPONSE TEAM STRUCTURE

1. The IRT shall consist of:

a) Chief Security Architect (Team Lead)

b) VP of Engineering (Technical Lead)

c) Chief Technology Officer

d) General Counsel

e) Client Services Director

f) Communications Director

2. Additional subject matter experts may be activated based on incident classification and scope.

4. INCIDENT CLASSIFICATION AND ESCALATION

1. Severity Levels:

- Level 1: Minor impact, localized effect
- Level 2: Moderate impact, potential client exposure
- Level 3: Significant impact, multiple systems affected
- Level 4: Critical impact, threat to core infrastructure

2. Escalation Protocol:

a) Level 1: Team Lead notification within 4 hours

b) Level 2: Executive notification within 2 hours

c) Level 3: CEO notification within 1 hour

d) Level 4: Immediate full team activation

5. RESPONSE PROCEDURES

1. Initial Assessment

a) Incident verification and scope determination

b) System isolation and containment measures

c) Evidence preservation protocols

d) Initial impact analysis

2. Containment and Eradication

a) Implementation of emergency response measures

b) Deployment of specialized OT security protocols

c) Execution of threat hunting procedures

d) System restoration planning

3. Client Communication

a) Notification requirements assessment

b) Regular status updates

c) Impact mitigation strategies

d) Recovery timeline communication

6. DOCUMENTATION AND REPORTING

1. The IRT shall maintain detailed incident logs including:

- Incident timeline
- Response actions taken
- System impact assessment
- Client communications
- Recovery measures implemented

2. Post-Incident Analysis

a) Root cause determination

b) Effectiveness evaluation

c) Procedure improvement recommendations

d) Lessons learned documentation

7. TESTING AND MAINTENANCE

1. This Plan shall be tested quarterly through:

- Tabletop exercises
- Technical simulations
- Cross-functional drills
- Client-involved scenarios

2. Annual Review Requirements

- Full Plan evaluation
- Update of contact information
- Integration of new threats
- Procedure optimization

8. COMPLIANCE AND REGULATORY REQUIREMENTS

1. This Plan adheres to:

- NIST Cybersecurity Framework

- ISO 27001 standards
- Maritime cybersecurity regulations
- Industry-specific compliance requirements

9. CONFIDENTIALITY

1. All incident-related information shall be treated as strictly confidential and shared only on a need-to-know basis.

2. External communications must be approved by Legal and Communications teams.

10. AUTHORIZATION

This Plan is authorized and approved by:

Dr. Marcus Chen
Chief Executive Officer
DeepShield Systems, Inc.

Sarah Blackwood
Chief Technology Officer
DeepShield Systems, Inc.

Date: January 15, 2024

REVISION HISTORY

Version 2.4 - January 15, 2024
- Updated IRT structure
- Enhanced maritime security protocols
- Revised escalation procedures

Version 2.3 - July 1, 2023
- Added OT-specific response procedures
- Updated compliance requirements