DISASTER RECOVERY PLAN - MARITIME OPERATIONS

DeepShield Systems, Inc.

Document Version: 2.4

Effective Date: January 15, 2024

Classification: Confidential

1. INTRODUCTION

1 This Disaster Recovery Plan ("Plan") establishes protocols and procedures for maintaining business continuity of DeepShield Systems, Inc.'s ("Company") maritime operations in the event of service disruptions, system failures, or catastrophic events affecting operational technology (OT) environments under protection.

2 This Plan specifically addresses maritime infrastructure security operations, including SCADA systems, vessel monitoring networks, port facility control systems, and offshore platform security infrastructure.

2. SCOPE AND APPLICABILITY

1 This Plan applies to all maritime-related operations, including:

a) Subsea infrastructure monitoring systems

b) Port facility security networks

c) Vessel tracking and control systems

d) Maritime OT security platforms

e) Offshore installation protection systems

2 Geographic Coverage: All maritime operations in North American waters, European territorial waters, and international waters where Company systems are deployed.

3. CRITICAL SYSTEMS IDENTIFICATION

1 Priority Level 1 Systems:

- DeepShield Maritime Control Center (DMCC)
- Vessel Security Operations Platform (VSOP)
- Maritime Threat Detection Network (MTDN)

- Emergency Response Communication System (ERCS)

2 Priority Level 2 Systems:

- Port Access Control Systems
- Automated Vessel Monitoring
- Subsea Sensor Networks
- Maritime Data Analytics Platform

4. RECOVERY TIME OBJECTIVES (RTO)

1 Priority Level 1 Systems: 4 hours maximum downtime

2 Priority Level 2 Systems: 12 hours maximum downtime

3 Supporting Systems: 24 hours maximum downtime

5. EMERGENCY RESPONSE PROCEDURES

1 Initial Assessment Protocol

a) Incident Commander shall assess system impact within 15 minutes

b) Emergency Response Team activation within 30 minutes

c) Stakeholder notification within 60 minutes

2 Communication Protocol

a) Primary: Secure Satellite Communication Network

b) Secondary: Encrypted Maritime Radio Network

c) Tertiary: Land-based Cellular Network

6. RECOVERY PROCEDURES

1 System Restoration Sequence:

1) Emergency Communication Systems

2) Threat Detection Networks

3) Control Systems

4) Monitoring Platforms

5) Analytics Systems

2 Data Recovery Protocol:

a) Access redundant data centers in Virginia and Singapore

b) Implement failover procedures per Document DS-OPS-317

c) Verify data integrity using DeepShield Verification Protocol

7. BACKUP FACILITIES AND RESOURCES

1 Primary Backup Operations Center:

- Location: Norfolk, Virginia
- Activation Time: 2 hours
- Capacity: 100% of critical operations

2 Secondary Backup Operations Center:

- Location: Singapore
- Activation Time: 4 hours
- Capacity: 75% of critical operations

8. TESTING AND MAINTENANCE

1 Testing Schedule:

- Quarterly tabletop exercises
- Semi-annual full-scale simulation
- Annual comprehensive system recovery test

2 Plan Updates:

- Quarterly review of procedures
- Annual comprehensive revision
- Post-incident assessment and modification

9. COMPLIANCE AND REPORTING

1 Regulatory Requirements:

- IMO Cybersecurity Guidelines
- MTSA Security Requirements
- EU NIS Directive

- NIST Cybersecurity Framework

2 Documentation Requirements:

- Incident logs maintained for 7 years
- Recovery action reports filed within 24 hours
- Compliance verification within 48 hours

10. LEGAL AND LIABILITY

1 This Plan is confidential and proprietary to DeepShield Systems, Inc.

2 Implementation of this Plan does not guarantee prevention of all service disruptions or system failures.

3 Company maintains cyber liability insurance per Policy #CYB-2024-789123.

11. 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

End of Document