BUSINESS CONTINUITY PLAN - SECURITY OPERATIONS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: Confidential

1. INTRODUCTION

1. This Business Continuity Plan for Security Operations ("Plan") establishes the procedures and protocols for maintaining continuous security operations at DeepShield Systems, Inc. ("Company") in the event of business disruption, system failure, or security incident.

2. This Plan specifically addresses the continuity of the Company's Security Operations Center (SOC) and related industrial control system (ICS) security monitoring services provided to clients.

2. SCOPE AND APPLICABILITY

1. This Plan applies to all security operations personnel, infrastructure, and systems supporting the Company's industrial cybersecurity platform and client-facing services.

2. Critical systems covered include:

a) Primary SOC facility (Delaware)

b) Backup SOC facility (Texas)

c) Industrial Control System Security Platform (ICSSP)

d) Maritime Security Operations Platform (MSOP)

e) Client-facing monitoring and response systems

f) Threat intelligence infrastructure

3. ROLES AND RESPONSIBILITIES

1. Security Operations Leadership:

- Chief Security Architect
- SOC Director
- Incident Response Team Lead
- Platform Operations Manager

2. Emergency Response Team:

- Primary Team (Alpha): 6 security analysts
- Secondary Team (Beta): 6 security analysts
- Engineering Support: 3 senior engineers
- Client Communications: 2 account managers

4. CRITICAL FUNCTION PRESERVATION

1. Priority Services:

a) Real-time threat monitoring

b) Industrial network security

c) Maritime infrastructure protection

d) Incident response capabilities

e) Client alert notifications

f) Regulatory compliance monitoring

2. Recovery Time Objectives (RTO):

- Critical monitoring systems: 15 minutes
- Threat detection capabilities: 30 minutes
- Client communications: 1 hour
- Full operational capability: 4 hours

5. ACTIVATION PROCEDURES

1. Plan Activation Triggers:

- Primary facility failure
- Cyber attack on Company infrastructure
- Natural disaster
- Physical security breach
- Critical system failure
- Personnel unavailability

2. Activation Authority:

- Chief Security Architect

- SOC Director (alternate)
- CEO (ultimate authority)

6. CONTINUITY PROCEDURES

1. Facility Failover:

a) Immediate transfer to backup SOC

b) Activation of redundant systems

c) Personnel relocation protocols

d) Communications redirect

2. System Recovery:

a) Implementation of redundant infrastructure

b) Data synchronization procedures

c) Client service restoration

d) Compliance monitoring reinstatement

7. COMMUNICATION PROTOCOLS

1. Internal Communications:

- Emergency notification system
- Secure messaging platform
- Backup communication channels
- Management escalation procedures

2. External Communications:

- Client notification procedures
- Regulatory reporting requirements
- Vendor coordination protocols
- Public relations management

8. TESTING AND MAINTENANCE

1. Testing Schedule:

- Quarterly failover tests

- Monthly communication tests
- Semi-annual full recovery exercise
- Annual plan review and update

2. Documentation Requirements:
- Test results and metrics
- Improvement recommendations
- Updated contact information
- Revised procedures

9. COMPLIANCE AND REPORTING

1. Regulatory Requirements:
- NIST Framework alignment
- ISO 27001 compliance
- Maritime security regulations
- Critical infrastructure requirements

2. Documentation:
- Incident logs
- Recovery metrics
- Compliance reports
- Test results

10. CONFIDENTIALITY

1. This Plan contains confidential and proprietary information of DeepShield Systems, Inc. and shall not be disclosed to any third party without written authorization from the Company's Chief Security Architect or General Counsel.

11. APPROVAL AND MAINTENANCE

1. This Plan shall be reviewed and updated annually or upon significant changes to operations, infrastructure, or regulatory requirements.

2. All revisions must be approved by:

- Chief Security Architect
- Chief Technology Officer
- General Counsel

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024

[Name]

General Counsel

Date: January 15, 2024