BUSINESS CONTINUITY PLAN COMPLIANCE REVIEW

DeepShield Systems, Inc.

Date: January 11, 2024

Document Reference: BCP-2024-001

1. EXECUTIVE SUMMARY

This Business Continuity Plan ("BCP") Compliance Review documents DeepShield Systems, Inc.'s ("Company") adherence to regulatory requirements and industry standards for business continuity and disaster recovery, with particular focus on the Company's role as a critical infrastructure cybersecurity provider.

2. SCOPE OF REVIEW

1. This review encompasses:

a) Primary business operations at Company headquarters (Delaware)

b) Secondary operations centers (Houston, TX and Seattle, WA)

c) Cloud infrastructure and backup facilities

d) Critical client-facing systems and services

e) Internal development and testing environments

2. Review Period: January 1, 2023 - December 31, 2023

3. REGULATORY FRAMEWORK COMPLIANCE

1. Federal Requirements

- NIST Cybersecurity Framework v1.1
- FERC Order No. 850 (CIP Reliability Standards)
- DHS Critical Infrastructure Protection Act requirements

2. Industry Standards

- ISO 22301:2019 (Business Continuity Management)
- ISO 27031 (ICT Readiness for Business Continuity)
- ISA/IEC 62443 (Industrial Automation and Control Systems Security)

4. CRITICAL SYSTEMS ASSESSMENT

1. Tier 1 Systems (Recovery Time Objective < 4 hours)

- DeepShield OT Monitoring Platform
- Maritime Defense Module
- SCADA Protection System
- Client Emergency Response Interface

2. Tier 2 Systems (Recovery Time Objective < 12 hours)

- Development Environment
- Customer Support Portal
- Internal Communications Systems
- Threat Intelligence Database

5. BUSINESS CONTINUITY MEASURES

1. Data Backup and Recovery

- Real-time replication to geographically distributed locations
- Daily incremental backups with 30-day retention
- Monthly full system backups with 12-month retention
- Quarterly recovery testing protocols

2. Alternative Operating Locations

- Primary: Delaware HQ (New Castle County)
- Secondary: Houston Operations Center
- Tertiary: Seattle Technical Center
- Remote Work Capability: 100% workforce enabled

6. INCIDENT RESPONSE PROTOCOLS

1. Emergency Response Team

- Chief Security Architect (Lead)
- VP of Engineering (Technical Operations)
- Director of Client Services (Customer Communications)

- Compliance Officer (Regulatory Reporting)

2. Communication Procedures

- Automated alert system for critical incidents
- Secure communication channels for response coordination
- Client notification protocols based on service level agreements
- Regulatory reporting procedures

7. TESTING AND VALIDATION

1. Testing Schedule

- Monthly: Critical system failover tests
- Quarterly: Full disaster recovery simulation
- Semi-annual: Business continuity exercise
- Annual: Third-party audit and assessment

2. Documentation Requirements

- Test results and metrics
- Improvement recommendations
- Implementation timelines
- Compliance verification

8. COMPLIANCE FINDINGS

1. Current Status

- Full compliance with federal requirements
- ISO 22301:2019 certification maintained
- Successfully completed all scheduled tests
- Zero critical findings in latest audit

2. Areas for Enhancement

- Enhance automation of failover procedures
- Implement additional redundancy for maritime modules
- Strengthen cross-facility coordination

- Update documentation for new service offerings

9. CERTIFICATION

The undersigned hereby certifies that this Business Continuity Plan Compliance Review accurately reflects DeepShield Systems, Inc.'s current business continuity status and compliance position as of the date hereof.

REVIEWED AND APPROVED BY:

```

_

Dr. Marcus Chen

Chief Executive Officer

Date: January 11, 2024

_

Robert Kessler

Chief Financial Officer

Date: January 11, 2024

_

Dr. Elena Rodriguez

Chief Security Architect

Date: January 11, 2024
```

10. LEGAL DISCLAIMER