CRISIS MANAGEMENT TEAM HANDBOOK

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

1. INTRODUCTION AND PURPOSE

1. This Crisis Management Team Handbook ("Handbook") establishes the operational framework and protocols for DeepShield Systems, Inc.'s ("Company") Crisis Management Team ("CMT") in responding to critical incidents affecting the Company's operations, clients, or infrastructure.

2. This document is classified as CONFIDENTIAL and is subject to the Company's Information Security Policy.

2. CRISIS MANAGEMENT TEAM COMPOSITION

1. Core Team Members

- Chief Executive Officer (CMT Leader)
- Chief Technology Officer (Technical Response Lead)
- Chief Security Architect (Security Operations Lead)
- Chief Financial Officer (Financial/Legal Response Lead)
- VP of Engineering (Infrastructure Response Lead)
- Director of Communications (Communications Lead)

2. Extended Support Team

- Regional Operations Directors
- Human Resources Director
- Legal Counsel
- Client Success Leaders
- Security Operations Center Manager

3. CRISIS CLASSIFICATION AND ACTIVATION

1. Crisis Levels

- Level 1: Localized Incident (Single client/system impact)

- Level 2: Multiple System Impact (Regional/service disruption)
- Level 3: Critical Infrastructure Impact (Multi-regional/severe disruption)
- Level 4: Enterprise-Wide Crisis (Catastrophic impact)

2. Activation Protocols

a) Initial assessment by Security Operations Center

b) Notification to CMT Leader

c) Team activation via secure communication channels

d) Assembly at designated command center (physical/virtual)

4. RESPONSE PROCEDURES

1. Initial Response (0-2 Hours)

- Incident verification and classification
- CMT activation and assembly
- Preliminary impact assessment
- Client notification protocols initiation
- Regulatory compliance review

2. Tactical Response (2-24 Hours)

- Technical containment measures
- Client impact mitigation
- Stakeholder communications
- Evidence preservation
- Resource allocation

3. Strategic Response (24+ Hours)

- Long-term recovery planning
- Business continuity implementation
- External communications strategy
- Legal/regulatory response coordination
- Financial impact assessment

5. COMMUNICATION PROTOCOLS

1. Internal Communications

- Secure messaging platform: DeepShield Emergency Response System
- Backup channels: Encrypted mobile communications
- Documentation requirements: All communications logged and timestamped

2. External Communications

- Client notifications per service level agreements
- Regulatory body notifications as required
- Media relations protocols
- Stakeholder updates

6. DOCUMENTATION AND REPORTING

1. Required Documentation

- Incident logs
- Response timeline
- Decision records
- Resource allocation tracking
- Communications records

2. Post-Incident Reports

- Technical impact assessment
- Client impact summary
- Financial impact analysis
- Regulatory compliance verification
- Lessons learned documentation

7. RECOVERY AND CONTINUITY

1. Business Continuity Integration

- Alignment with Business Continuity Plan
- Service restoration priorities
- Resource reallocation procedures
- Client service recovery protocols

2. Post-Crisis Review

- Response effectiveness evaluation
- Protocol update recommendations
- Training requirement identification
- Documentation updates

8. LEGAL AND COMPLIANCE

1. Legal Considerations

- Evidence preservation requirements
- Attorney-client privilege protocols
- Regulatory reporting obligations
- Liability mitigation measures

2. Compliance Requirements

- Industry-specific regulations
- Data protection standards
- Critical infrastructure requirements
- Documentation retention policies

9. MAINTENANCE AND TRAINING

1. Regular Review and Updates

- Quarterly handbook review
- Annual comprehensive update
- Protocol testing and validation
- Team composition updates

2. Training Requirements

- Quarterly tabletop exercises
- Annual full-scale simulation
- Role-specific training
- New member orientation

10. CONFIDENTIALITY AND DISTRIBUTION

This document contains confidential and proprietary information of DeepShield Systems, Inc. Distribution is restricted to authorized Crisis Management Team members and designated support personnel. Unauthorized disclosure is prohibited.

APPROVAL AND REVISION HISTORY

Version 2.4

Approved by: Board of Directors

Date: January 15, 2024

Previous Revisions:

- Version 2.3: July 15, 2023
- Version 2.2: January 15, 2023
- Version 2.1: July 15, 2022
- Version 2.0: January 15, 2022

–

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

–

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.