EMERGENCY RESPONSE PROTOCOL - CYBER INCIDENTS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Emergency Response Protocol ("Protocol") establishes mandatory procedures for responding to cybersecurity incidents affecting DeepShield Systems, Inc.'s ("Company") operations, customer environments, or critical infrastructure protection systems.

2. This Protocol applies to all Company employees, contractors, and authorized third parties who access or manage Company systems or customer deployments.

2. DEFINITIONS

1. "Cyber Incident" means any actual or suspected unauthorized access, breach, exploitation, or disruption of Company systems, customer environments, or protected infrastructure.

2. "Critical Systems" means the Company's core security platform, customer-facing services, and operational technology (OT) protection infrastructure.

3. "Response Team" means the designated group of Company personnel responsible for incident management, as defined in Section 4.

3. INCIDENT CLASSIFICATION

1. Level 1 - Minor Impact

- Isolated system anomalies
- Non-critical service disruptions
- Response Time: Within 4 hours

2. Level 2 - Moderate Impact

- Multiple system compromises
- Customer service degradation

- Response Time: Within 2 hours

3. Level 3 - Critical Impact

- Active breach of critical systems
- Customer data compromise
- Infrastructure protection failure
- Response Time: Immediate (15 minutes)

4. RESPONSE TEAM STRUCTURE

1. Primary Response Team

- Chief Security Architect (Team Lead)
- VP of Engineering
- Senior Security Operations Manager
- Customer Success Director
- Legal Counsel

2. Extended Response Team

- CEO
- CTO
- CFO
- Communications Director
- Regional Technical Directors

5. INCIDENT RESPONSE PROCEDURES

1. Initial Detection and Assessment

a) Document incident discovery time and source

b) Perform preliminary impact assessment

c) Assign incident classification level

d) Activate appropriate response team members

2. Containment Measures

a) Isolate affected systems

b) Implement emergency access controls

c) Deploy countermeasures

d) Document all containment actions

3. Customer Communication

a) Notify affected customers within timeframes specified in service agreements

b) Provide interim status updates every 2 hours

c) Document all customer communications

4. Recovery Operations

a) Validate system integrity

b) Restore affected services

c) Implement additional security controls

d) Verify protection mechanisms

6. DOCUMENTATION REQUIREMENTS

1. Incident Reports must include:

- Incident timeline
- Systems affected
- Customer impact assessment
- Response actions taken
- Recovery measures implemented
- Root cause analysis
- Preventive recommendations

2. All documentation must be preserved for minimum 7 years.

7. REGULATORY COMPLIANCE

1. Response actions must comply with:

- NIST Cybersecurity Framework
- ISO 27001 requirements
- Customer contractual obligations

- Industry-specific regulations

2. Notification requirements per jurisdiction must be tracked and fulfilled.

8. POST-INCIDENT PROCEDURES

1. After-Action Review

- Conduct within 48 hours of resolution
- Document lessons learned
- Update response procedures
- Implement preventive measures

2. Training Updates

- Revise training materials
- Conduct refresher sessions
- Update simulation exercises

9. PROTOCOL MAINTENANCE

1. This Protocol shall be reviewed quarterly and updated as needed.

2. Changes require approval from:

- Chief Security Architect
- VP of Engineering
- Legal Counsel

10. CONFIDENTIALITY

1. This Protocol and all incident-related information are strictly confidential.

2. Disclosure restricted to authorized personnel on need-to-know basis.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 15th day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

James Morrison

VP of Engineering

By:

[Legal Counsel Name]

General Counsel