EMERGENCY RESPONSE PLAN: CYBER INCIDENTS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 3.2

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Emergency Response Plan for Cyber Incidents ("Plan") establishes the procedures and protocols for responding to cybersecurity incidents affecting DeepShield Systems, Inc.'s ("Company") operations, client systems, or protected infrastructure.

2. This Plan applies to all employees, contractors, and third-party service providers who have access to Company systems or client operational technology (OT) environments.

2. DEFINITIONS

1. "Cyber Incident" means any actual or suspected event that threatens the confidentiality, integrity, or availability of Company or client information systems, industrial control systems (ICS), or operational technology (OT) environments.

2. "Critical Infrastructure" means systems, networks, and assets designated as essential to client operations or national security as defined under applicable regulations.

3. "Incident Response Team" or "IRT" means the cross-functional team responsible for managing cyber incident response activities.

3. INCIDENT RESPONSE TEAM COMPOSITION

1. The IRT shall consist of:

a) Chief Security Architect (Team Lead)

b) VP of Engineering

c) Senior Network Security Engineer

d) OT Systems Specialist

e) Legal Counsel

f) Client Communications Manager

2. Additional members may be activated based on incident severity and scope.

4. INCIDENT CLASSIFICATION AND ESCALATION

1. Severity Levels:

- Level 1: Minor impact, single system affected
- Level 2: Moderate impact, multiple systems affected
- Level 3: Major impact, critical systems compromised
- Level 4: Severe impact, widespread system failure or data breach

2. Escalation Protocol:

a) Level 1: Team Lead notification within 2 hours

b) Level 2: Executive notification within 1 hour

c) Level 3: CEO notification within 30 minutes

d) Level 4: Immediate Board and stakeholder notification

5. RESPONSE PROCEDURES

1. Initial Assessment

a) Identify affected systems and scope of impact

b) Document initial findings and timestamp all activities

c) Establish secure communications channel

d) Activate required IRT members

2. Containment

a) Isolate affected systems

b) Implement emergency access controls

c) Deploy countermeasures per DeepShield Security Protocol DS-7.3

d) Preserve evidence for forensic analysis

3. Client Protection Measures

a) Activate client system safeguards

b) Deploy emergency OT protection protocols

c) Implement fail-safe mechanisms

d) Monitor secondary systems for cascade effects

6. COMMUNICATION PROTOCOLS

1. Internal Communications

a) Use encrypted communication channels

b) Follow predetermined notification hierarchy

c) Maintain detailed incident logs

d) Document all response actions

2. External Communications

a) Client notification per service level agreements

b) Regulatory reporting as required by law

c) Law enforcement contact if necessary

d) Media relations through authorized spokespersons only

7. RECOVERY AND RESTORATION

1. System Recovery

a) Implement recovery procedures per affected system

b) Verify system integrity before restoration

c) Deploy enhanced monitoring tools

d) Document recovery steps

2. Post-Incident Activities

a) Conduct root cause analysis

b) Update security measures based on findings

c) Revise response procedures as needed

d) Prepare incident report

8. COMPLIANCE AND DOCUMENTATION

1. All incident response activities must comply with:

a) Federal cybersecurity regulations

b) Industry standards (NIST, ISO 27001)

c) Client contractual requirements

d) Company security policies

2. Required Documentation:

a) Incident timeline and response actions

b) System logs and forensic data

c) Communication records

d) Recovery procedures implemented

9. TRAINING AND MAINTENANCE

1. The IRT shall conduct quarterly incident response drills.

2. This Plan shall be reviewed and updated annually or after major incidents.

10. LEGAL DISCLAIMERS

This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure or distribution is prohibited. This Plan does not guarantee prevention or successful resolution of cyber incidents. The Company reserves the right to modify these procedures as necessary.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by the Board of Directors of DeepShield Systems, Inc.

Date: January 15, 2024

_

Dr. Marcus Chen

Chief Executive Officer

_

Dr. Elena Rodriguez

Chief Security Architect

_

Robert Kessler

Chief Financial Officer