DATA BREACH RESPONSE PROTOCOL

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

1. PURPOSE AND SCOPE

1. This Data Breach Response Protocol ("Protocol") establishes mandatory procedures for responding to actual or suspected data breaches affecting DeepShield Systems, Inc. ("Company") or its clients' industrial control systems (ICS), operational technology (OT) environments, or related critical infrastructure.

2. This Protocol applies to all Company employees, contractors, and third-party service providers who have access to Company systems or client environments.

2. DEFINITIONS

1. "Data Breach" means any unauthorized access, acquisition, use, modification, disclosure, or destruction of protected data, including but not limited to:

a) Client ICS configurations and security parameters

b) SCADA network architectures and vulnerabilities

c) Maritime and subsea infrastructure protection systems

d) Proprietary deep-layer security algorithms

e) Client operational data and system logs

2. "Response Team" means the cross-functional team responsible for implementing this Protocol, consisting of:

a) Chief Security Architect (Team Lead)

b) Chief Technology Officer

c) VP of Engineering

d) General Counsel

e) Client Success Director

f) Incident Response Engineers

3. IMMEDIATE RESPONSE PROCEDURES

1. Initial Detection and Assessment

a) Any person who discovers or suspects a Data Breach must immediately notify the Response Team through the Secure Incident Reporting System (SIRS).

b) The Response Team shall convene within 30 minutes of notification during business hours or within 2 hours during non-business hours.

c) Initial assessment must determine:

- Scope and nature of the breach
- Systems and clients affected
- Current breach status (ongoing/contained)
- Immediate risk to critical infrastructure

2. Containment Measures

a) Implement immediate technical countermeasures to isolate affected systems

b) Activate emergency shutdown procedures if critical infrastructure is at risk

c) Suspend compromised access credentials

d) Deploy adaptive defense mechanisms to prevent breach expansion

4. NOTIFICATION REQUIREMENTS

1. Client Notification

a) Affected clients must be notified within:

- 1 hour for critical infrastructure breaches
- 4 hours for high-severity breaches
- 24 hours for medium-severity breaches

b) Notifications must include:

- Breach description and known impact
- Containment measures implemented
- Recommended client actions
- Dedicated incident response contact

2. Regulatory Notification

a) Legal department to assess notification obligations under:

- State breach notification laws
- Federal regulations (CISA, NERC-CIP, etc.)
- International requirements (GDPR, etc.)

b) File required notifications within mandatory timeframes

c) Maintain documentation of all notifications

5. INVESTIGATION AND DOCUMENTATION

1. Technical Investigation

a) Preserve all relevant logs and forensic data

b) Document breach vector and methodology

c) Identify all compromised systems and data

d) Determine duration and scope of unauthorized access

e) Assess effectiveness of existing security controls

2. Root Cause Analysis

a) Conduct comprehensive system audit

b) Review relevant security policies and procedures

c) Identify contributing factors and control failures

d) Document findings in formal incident report

6. REMEDIATION AND RECOVERY

1. System Recovery

a) Implement required security patches and updates

b) Restore systems from verified backups

c) Reset all potentially compromised credentials

d) Verify integrity of restored systems

e) Document all recovery actions

2. Enhanced Security Measures

a) Deploy additional monitoring and controls

b) Update security policies and procedures

c) Conduct targeted security training

d) Implement identified security improvements

7. POST-INCIDENT REVIEW

1. The Response Team shall conduct a post-incident review within 72 hours of breach resolution, addressing:

a) Effectiveness of response procedures

b) Communication effectiveness

c) Required policy/procedure updates

d) Preventive measure recommendations

2. Prepare detailed incident report for executive management including:

a) Incident timeline and impact assessment

b) Response effectiveness evaluation

c) Recommended security improvements

d) Updated risk assessment

8. PROTOCOL MAINTENANCE

1. This Protocol shall be reviewed and updated annually or following any significant security incident.

2. All updates must be approved by the Chief Security Architect and General Counsel.

9. COMPLIANCE AND ENFORCEMENT

1. Compliance with this Protocol is mandatory for all covered persons.

2. Violations may result in disciplinary action up to and including termination.

Approved by:

Dr. Elena Rodriguez

Chief Security Architect

Date:

General Counsel

Date: