INCIDENT REPORTING COMPLIANCE PROCEDURE

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: DSS-IRP-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Incident Reporting Compliance Procedure ("Procedure") establishes mandatory protocols for reporting cybersecurity incidents, operational technology (OT) anomalies, and security breaches affecting DeepShield Systems, Inc. ("Company") and its clients' industrial control systems (ICS).

2. This Procedure applies to all Company employees, contractors, and authorized third parties who access, operate, or maintain the Company's cybersecurity platforms and client installations.

2. DEFINITIONS

1. "Critical Incident" means any event that:

a) Compromises the integrity of protected industrial systems

b) Disrupts operational technology environments

c) Triggers automated incident response mechanisms

d) Results in unauthorized access to SCADA networks

e) Affects maritime or subsea infrastructure security components

2. "Reportable Event" means any occurrence that meets the thresholds defined in Section 4 of this Procedure.

3. "Response Team" means the designated group of Company personnel responsible for incident assessment and response coordination.

3. INCIDENT CLASSIFICATION

1. Level 1 - Critical Infrastructure Impact

- Direct compromise of critical infrastructure systems
- Widespread disruption to industrial operations

- Confirmed breach of deep-layer security architecture

2. Level 2 - Significant Security Events

- Attempted unauthorized access to protected systems
- Detection of advanced persistent threats
- Multiple correlated security anomalies

3. Level 3 - Security Anomalies

- Single-point security alerts
- System performance irregularities
- Non-critical compliance violations

4. REPORTING REQUIREMENTS

1. Immediate Reporting (Within 1 Hour)

- All Level 1 incidents
- Confirmed breaches of client systems
- Maritime security system compromises
- Critical infrastructure protection failures

2. Priority Reporting (Within 4 Hours)

- Level 2 incidents
- Multiple related security events
- Suspected advanced persistent threats
- System integrity violations

3. Standard Reporting (Within 24 Hours)

- Level 3 incidents
- Routine security anomalies
- Compliance monitoring alerts
- System performance issues

5. REPORTING PROCEDURES

1. Initial Notification

a) Contact the Security Operations Center (SOC) at [INTERNAL NUMBER]

b) Submit preliminary incident report via the Incident Management Portal

c) Notify immediate supervisor and relevant department heads

d) Document initial response actions taken

2. Documentation Requirements

a) Incident classification and severity level

b) Systems and components affected

c) Timeline of detected events

d) Initial impact assessment

e) Client facilities involved (if applicable)

f) Preliminary root cause analysis

g) Immediate mitigation measures implemented

3. Escalation Protocol

a) Chief Security Architect review for Level 1 incidents

b) VP of Engineering notification for client-impacting events

c) CEO and Executive Team briefing for critical infrastructure compromises

d) Legal Department consultation for compliance implications

6. REGULATORY COMPLIANCE

1. External Reporting Obligations

- CISA 24-hour notification requirements
- SEC material cybersecurity incident disclosure
- Maritime cybersecurity reporting requirements
- State-specific breach notification laws
- International reporting obligations

2. Documentation Retention

- Incident reports maintained for 7 years
- Investigation records preserved per legal requirements
- Audit trails secured in encrypted storage

- Client notification records archived

7. CLIENT NOTIFICATION

1. Notification Triggers

- Confirmed compromise of client systems
- Potential exposure of client data
- Service interruptions exceeding 15 minutes
- Security events affecting multiple clients

2. Communication Protocol

a) Initial client notification within defined SLA timeframes

b) Regular status updates during incident response

c) Post-incident summary and remediation report

d) Executive briefing for significant events

8. REVIEW AND UPDATES

1. This Procedure shall be reviewed annually by the Chief Security Architect and Legal Department.

2. Updates require approval from:

- Chief Security Architect
- VP of Engineering
- Chief Technology Officer
- General Counsel

9. COMPLIANCE AND ENFORCEMENT

1. Failure to comply with this Procedure may result in disciplinary action up to and including termination of employment or service agreements.

2. The Company reserves the right to modify this Procedure at any time to ensure compliance with applicable laws and regulations.

APPROVAL AND REVISION HISTORY

Document Owner: Dr. Elena Rodriguez, Chief Security Architect

Last Review Date: January 15, 2024

Next Review Date: January 15, 2025

Approved by:

- Dr. Marcus Chen, CEO
- Sarah Blackwood, CTO
- James Morrison, VP of Engineering
- Dr. Elena Rodriguez, Chief Security Architect

Version History:

- 2.0: January 15, 2024 - Comprehensive update incorporating maritime security requirements
- 1.1: June 10, 2023 - Updated regulatory compliance section
- 1.0: March 1, 2023 - Initial release