SECURITY INCIDENT CLASSIFICATION MATRIX

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document ID: SEC-ICM-2024-001

Version: 3.0

1. PURPOSE AND SCOPE

1. This Security Incident Classification Matrix ("Matrix") establishes standardized criteria for categorizing and responding to security incidents affecting DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security solutions, operational technology (OT) environments, and related critical infrastructure protection services.

2. This Matrix applies to all security incidents involving:

a) Company's proprietary deep-layer security architecture

b) Customer OT/ICS environments under Company protection

c) Maritime and subsea infrastructure security systems

d) SCADA networks and industrial automation systems

e) Related monitoring and defense mechanisms

2. INCIDENT SEVERITY LEVELS

1. **Level 1 - Critical**

- Complete compromise of critical OT systems
- Unauthorized control of industrial processes
- Physical damage to protected infrastructure
- Life-threatening safety conditions
- Multi-customer service interruption
- Response Time: Immediate (15 minutes)

2. **Level 2 - High**

- Partial compromise of OT systems
- Unauthorized access to control interfaces
- Non-destructive system manipulation

- Single customer service interruption
- Potential safety implications
- Response Time: Urgent (1 hour)

3. **Level 3 - Medium**

- Detected intrusion attempts
- Anomalous system behavior
- Non-critical system alerts
- Performance degradation
- Limited scope impacts
- Response Time: Priority (4 hours)

4. **Level 4 - Low**

- Minor security events
- Failed access attempts
- System warnings
- Configuration issues
- No operational impact
- Response Time: Standard (24 hours)

3. INCIDENT RESPONSE PROTOCOLS

1. **Initial Assessment**

- Incident detection source verification
- Preliminary impact evaluation
- Severity level assignment
- Stakeholder notification requirements
- Response team activation

2. **Containment Procedures**

- Level 1: Full system isolation protocols
- Level 2: Targeted component quarantine
- Level 3: Enhanced monitoring mode

- Level 4: Standard security measures

3. **Escalation Matrix**

- Level 1: CEO, CTO, Chief Security Architect
- Level 2: VP Engineering, Security Operations
- Level 3: Security Team Lead
- Level 4: Security Analyst on Duty

4. REPORTING REQUIREMENTS

1. **Internal Reporting**

- Immediate notification to designated personnel
- Incident tracking system documentation
- Root cause analysis documentation
- Resolution verification report
- Lessons learned documentation

2. **Customer Notification**

- Level 1: Immediate verbal + written notice
- Level 2: Written notice within 2 hours
- Level 3: Written notice within 8 hours
- Level 4: Include in periodic reports

3. **Regulatory Reporting**

- Critical infrastructure notifications
- Industry compliance requirements
- Government agency reports
- Insurance carrier notification

5. DOCUMENTATION AND REVIEW

1. All security incidents shall be documented in the Company's Incident Management System, including:

a) Initial detection details

b) Response actions taken

c) Impact assessment

d) Resolution measures

e) Prevention recommendations

2. Post-Incident Review Requirements:

- Level 1: Full review within 24 hours
- Level 2: Review within 48 hours
- Level 3: Review within 5 business days
- Level 4: Monthly incident review

6. MATRIX MAINTENANCE

1. This Matrix shall be reviewed and updated annually or upon:

a) Significant technology changes

b) New threat identification

c) Regulatory requirement changes

d) Post-incident recommendations

2. All updates require approval from:

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

7. CONFIDENTIALITY

1. This Matrix contains confidential and proprietary information of DeepShield Systems, Inc. and shall not be disclosed to unauthorized parties.

8. APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 1st day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

Sarah Blackwood

Chief Technology Officer