DEEPSHIELD SECURITY INCIDENT CLASSIFICATION GUIDE

Document ID: SEC-ICG-2024-01

Effective Date: January 15, 2024

Version: 3.2

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Security Incident Classification Guide ("Guide") establishes the standardized framework for classifying and categorizing security incidents affecting DeepShield Systems, Inc.'s ("DeepShield") industrial control system (ICS) security infrastructure, operational technology (OT) environments, and related critical systems.

2. This Guide applies to all security incidents involving DeepShield's products, services, internal systems, and customer deployments, including but not limited to the DeepShield Maritime Shield(TM), SubSea Defender(TM), and Industrial Guardian(TM) platforms.

2. DEFINITIONS

1. "Security Incident" means any event that threatens the confidentiality, integrity, or availability of DeepShield's or its customers' systems, networks, or data.

2. "Critical Infrastructure" refers to systems, networks, and assets designated as essential under applicable regulatory frameworks including CISA, NERC-CIP, and maritime security regulations.

3. "OT Environment" means operational technology systems, including industrial control systems, SCADA networks, and process control devices.

3. INCIDENT SEVERITY LEVELS

1. **Level 1 - Critical**

- Direct compromise of critical infrastructure systems
- Unauthorized access to OT control systems
- Active exploitation of DeepShield security products
- Customer data breach affecting multiple installations

- System failures affecting maritime or subsea operations

2. **Level 2 - High**
- Attempted penetration of critical systems
- Denial of service affecting operational capabilities
- Advanced persistent threats (APT) detection
- Malware infection in protected environments
- Configuration changes causing security degradation

3. **Level 3 - Medium**
- Suspicious activity requiring investigation
- Minor security policy violations
- Non-critical system vulnerabilities
- Isolated anomaly detection alerts
- Limited scope authentication failures

4. **Level 4 - Low**
- Routine security events
- Failed access attempts within normal parameters
- Minor configuration issues
- Individual user policy violations
- System performance anomalies

4. RESPONSE REQUIREMENTS

1. **Critical (Level 1)**
- Immediate CEO and Board notification
- Response team activation within 15 minutes
- Customer notification within 1 hour
- Regulatory reporting as required by law
- Post-incident analysis within 24 hours

2. **High (Level 2)**
- CISO notification within 30 minutes

- Response team activation within 1 hour
- Customer notification within 4 hours
- Incident containment within 8 hours
- Root cause analysis within 48 hours

3. **Medium (Level 3)**
- Security team notification within 2 hours
- Investigation initiation within 4 hours
- Resolution within 24 hours
- Documentation within 48 hours

4. **Low (Level 4)**
- Standard ticket creation
- Resolution within 72 hours
- Monthly trend analysis review

5. DOCUMENTATION AND REPORTING

1. All security incidents must be documented in DeepShield's Secure Incident Management System (SIMS) including:
- Incident classification and severity
- Detection method and timeline
- Systems and assets affected
- Response actions taken
- Resolution status and measures
- Customer impact assessment

2. Required documentation retention periods:
- Level 1 incidents: 7 years
- Level 2 incidents: 5 years
- Level 3 incidents: 3 years
- Level 4 incidents: 1 year

6. CONFIDENTIALITY

1. All incident information shall be treated as strictly confidential and shared only on a need-to-know basis in accordance with DeepShield's Information Security Policy.

2. External communications regarding security incidents must be approved by Legal and Corporate Communications departments.

7. REVIEW AND UPDATES

1. This Guide shall be reviewed annually by the Security Operations Committee and updated as necessary to reflect evolving threats and operational requirements.

2. Material changes require approval from the Chief Security Architect and General Counsel.

8. COMPLIANCE

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

APPROVAL AND EXECUTION

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

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

Sarah Blackwood

Chief Technology Officer