SECURITY AWARENESS PROGRAM GUIDELINES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. These Security Awareness Program Guidelines ("Guidelines") establish the framework for DeepShield Systems, Inc.'s ("Company") comprehensive security awareness training program for all employees, contractors, and authorized third parties who access Company systems or information.

2. These Guidelines apply to all personnel regardless of role or location, with specific enhanced requirements for those handling critical infrastructure protection systems, industrial control systems (ICS), or operational technology (OT) environments.

2. DEFINITIONS

1. "Critical Systems" means any Company systems, networks, or applications that support industrial control systems, SCADA networks, or maritime infrastructure protection platforms.

2. "Security Incident" refers to any actual or suspected compromise, unauthorized access, or breach of Company systems, networks, or data.

3. "Training Period" means the recurring 12-month cycle during which all required security awareness training must be completed.

3. PROGRAM REQUIREMENTS

1. Mandatory Training Components

a) New Hire Orientation

- Initial security awareness training within 5 business days of start date
- Role-specific security protocols and procedures
- Critical infrastructure protection awareness
- Industrial cybersecurity fundamentals

b) Annual Refresher Training

- Updated threat landscape review
- Incident response procedures
- Social engineering awareness
- Regulatory compliance requirements

c) Quarterly Security Updates

- Emerging threat briefings
- Recent incident case studies
- Security policy changes
- Best practice updates

2. Specialized Training Requirements

a) OT Security Personnel

- Advanced ICS security protocols
- SCADA system protection
- Maritime infrastructure security
- Deep-layer architecture training

b) Development Team

- Secure coding practices
- API security protocols
- Threat modeling
- Security testing methodologies

4. DELIVERY AND DOCUMENTATION

1. Training Delivery Methods

a) Interactive online modules through Company learning management system

b) Instructor-led sessions for specialized topics

c) Hands-on workshops for technical personnel

d) Simulation exercises for incident response scenarios

2. Documentation Requirements

a) Training completion records maintained for 5 years

b) Quarterly compliance reports to Security Committee

c) Annual program effectiveness assessment

d) Certification tracking for specialized roles

5. COMPLIANCE AND ENFORCEMENT

1. Completion Requirements

a) All personnel must complete assigned training within designated timeframes

b) Failure to complete required training may result in system access suspension

c) Three consecutive missed training sessions trigger management review

d) Annual compliance rate must exceed 95% of eligible personnel

2. Assessment and Verification

a) Knowledge assessments required for each training module

b) Minimum passing score of 80% required

c) Maximum of three attempts per assessment

d) Remedial training required for failed attempts

6. PROGRAM GOVERNANCE

1. Oversight Responsibilities

a) Chief Security Architect: Program strategy and content approval

b) Security Training Coordinator: Program administration

c) Department Managers: Compliance monitoring

d) Human Resources: Record maintenance

2. Review and Updates

a) Annual program review by Security Committee

b) Quarterly content updates based on threat intelligence

c) Regulatory compliance verification

d) Effectiveness metrics assessment

7. CONFIDENTIALITY AND INTELLECTUAL PROPERTY

1. All training materials, documentation, and related content are confidential information of the Company and may not be shared with unauthorized parties.

2. Training materials incorporating Company's proprietary deep-layer security architecture are protected intellectual property and subject to additional confidentiality requirements.

8. MODIFICATIONS AND AMENDMENTS

1. These Guidelines may be modified or amended by the Company's Security Committee with approval from executive management.

2. Material changes will be communicated to all affected personnel with reasonable notice.

APPROVAL AND ADOPTION

These Guidelines have been reviewed and approved by:

Dr. Elena Rodriguez
Chief Security Architect
Date: January 15, 2024

Sarah Blackwood
Chief Technology Officer
Date: January 15, 2024