SECURITY AWARENESS TRAINING PROGRAM 2024

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 1.0

Classification: INTERNAL USE ONLY

1. PROGRAM OVERVIEW

1. This Security Awareness Training Program ("Program") establishes mandatory security awareness training requirements for all employees, contractors, and authorized users ("Personnel") of DeepShield Systems, Inc. ("Company") for the calendar year 2024.

2. This Program is designed to protect the Company's industrial control system (ICS) security solutions, operational technology (OT) environments, and related intellectual property while ensuring compliance with applicable cybersecurity regulations and industry standards.

2. SCOPE AND APPLICABILITY

1. This Program applies to:

a) All full-time and part-time employees

b) Independent contractors and consultants

c) Temporary workers and interns

d) Third-party service providers with access to Company systems

e) Board members and executive officers

2. Training requirements are tailored based on role classification:

- Tier 1: General Personnel
- Tier 2: Technical Staff
- Tier 3: Security Operations
- Tier 4: Executive Leadership

3. MANDATORY TRAINING MODULES

1. Core Security Modules (All Personnel):

a) Industrial Cybersecurity Fundamentals

b) Social Engineering and Phishing Prevention

c) Secure Remote Access Protocols

d) Data Classification and Handling

e) Incident Reporting Procedures

2. Role-Specific Modules:

a) OT Security Architecture (Technical Staff)

b) SCADA Network Protection (Security Operations)

c) Maritime Infrastructure Security (Project Teams)

d) Advanced Threat Detection (Security Operations)

e) Regulatory Compliance Training (Leadership)

4. TRAINING DELIVERY AND COMPLETION

1. Training Schedule:

- New hire training: Within 5 business days of start date
- Annual refresher: Q1 2024 completion required
- Quarterly updates: As released by Security Team
- Ad-hoc training: Following security incidents or policy changes

2. Delivery Methods:

- Interactive online learning management system
- Virtual instructor-led sessions
- Hands-on laboratory exercises
- Simulation-based assessments
- Department-specific workshops

5. COMPLIANCE AND ASSESSMENT

1. Completion Requirements:

a) Minimum passing score: 85%

b) Maximum of three attempts per assessment

c) Completion documentation maintained for 3 years

d) Annual certification of completion required

2. Non-Compliance Consequences:

a) System access suspension after 30 days overdue

b) Performance evaluation impact

c) Potential disciplinary action

d) Contractor agreement termination

6. SPECIALIZED REQUIREMENTS

1. Critical Infrastructure Teams:

- Monthly threat briefings
- Quarterly tabletop exercises
- Semi-annual penetration testing awareness
- Industry-specific compliance updates

2. Development and Engineering:

- Secure coding practices
- Supply chain security
- API security protocols
- Vulnerability management

7. PROGRAM ADMINISTRATION

1. Program Oversight:

- Chief Security Officer: Program authority
- Security Training Manager: Implementation
- Department Managers: Compliance monitoring
- HR: Record maintenance

2. Documentation Requirements:

- Training completion records
- Assessment results
- Attendance logs
- Certification status

8. MODIFICATIONS AND UPDATES

1. This Program shall be reviewed and updated:

- Annually at minimum
- Following major security incidents
- Upon significant technology changes
- As required by regulatory changes

2. All modifications require approval from:

- Chief Security Officer
- Chief Technology Officer
- Legal Department
- Executive Committee

9. LEGAL COMPLIANCE

1. This Program complies with:

- NIST Cybersecurity Framework
- ISO 27001 requirements
- Industry-specific regulations
- State and federal data protection laws

10. ATTESTATION

The undersigned hereby acknowledges review and approval of this Security Awareness Training Program for calendar year 2024.

APPROVED BY:

Dr. Marcus Chen

Chief Executive Officer

Date: December 15, 2023

Sarah Blackwood

Chief Technology Officer

Date: December 15, 2023

Dr. Elena Rodriguez

Chief Security Architect

Date: December 15, 2023