ANNUAL CYBERSECURITY TRAINING PROGRAM MATERIALS

DeepShield Systems, Inc.

Last Updated: January 1, 2024

Document ID: DSS-HR-CYB-2024-001

1. PROGRAM OVERVIEW

1. This Annual Cybersecurity Training Program ("Program") is established by DeepShield Systems, Inc. ("Company") to ensure compliance with industry standards, regulatory requirements, and internal security policies governing the protection of critical infrastructure and operational technology environments.

2. All employees, contractors, and authorized third-party personnel ("Participants") must complete this mandatory training program annually as a condition of continued access to Company systems and facilities.

2. TRAINING MODULES

1. Core Security Awareness

- Industrial Control System (ICS) Security Fundamentals
- SCADA Network Protection Protocols
- Maritime and Subsea Infrastructure Security
- Social Engineering and Phishing Prevention
- Incident Response Procedures

2. Role-Specific Training

- Engineering Team: Advanced OT Security Architecture
- Operations Team: Real-time Monitoring Protocols
- Development Team: Secure Coding Practices
- Client Services: Security Implementation Guidelines
- Management: Risk Assessment and Compliance

3. DELIVERY AND COMPLETION REQUIREMENTS

1. Training Format

- Online Learning Management System (LMS) modules
- Interactive simulation exercises
- Practical assessment scenarios
- Live instructor-led sessions for specialized topics
- Quarterly security updates and briefings

2. Completion Criteria

- Minimum score of 85% on all assessment modules
- Completion of all hands-on simulation exercises
- Signed acknowledgment of security policies
- Annual recertification requirement

4. CONFIDENTIALITY AND INTELLECTUAL PROPERTY

1. All training materials, including but not limited to presentations, documentation, simulations, and assessments, are confidential and proprietary to DeepShield Systems, Inc.

2. Participants shall not:

- Share or distribute training materials
- Record or reproduce training sessions
- Use materials outside of authorized training purposes
- Disclose specific security protocols or configurations

5. COMPLIANCE AND ENFORCEMENT

1. Regulatory Framework

- NIST Cybersecurity Framework
- IEC 62443 Industrial Security Standards
- Maritime Cybersecurity Guidelines
- Critical Infrastructure Protection Requirements

2. Documentation Requirements

- Training completion records maintained for 5 years
- Quarterly compliance reports to Security Committee
- Annual audit of training effectiveness

- Individual certification tracking

6. INCIDENT RESPONSE TRAINING

1. Practical Scenarios

- OT Network Breach Response
- Ransomware Attack Simulation
- Supply Chain Compromise
- Physical Security Integration
- Maritime Asset Protection

2. Response Protocols

- Immediate containment procedures
- Escalation pathways
- Documentation requirements
- Stakeholder communication
- Recovery processes

7. CERTIFICATION AND VALIDATION

1. Upon successful completion, participants receive:

- Annual Security Certification
- Role-specific competency validation
- System access authorization
- Compliance documentation

2. Certification Maintenance

- Quarterly knowledge assessments
- Participation in security drills
- Continuing education requirements
- Policy update acknowledgments

8. PROGRAM UPDATES AND REVISIONS

1. This Program shall be reviewed and updated:

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

9. LEGAL DISCLAIMER

This training program and associated materials are protected by copyright and trade secret laws. DeepShield Systems, Inc. reserves all rights not expressly granted herein. While this program is designed to enhance security awareness and compliance, completion does not guarantee against security incidents or constitute legal advice.

10. ACKNOWLEDGMENT

By participating in this training program, individuals acknowledge their understanding and agreement to comply with all security policies, procedures, and confidentiality requirements outlined herein.

Approved by:

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: _