TECHNICAL SKILLS ASSESSMENT FRAMEWORK

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Technical Skills Assessment Framework ("Framework") establishes the standardized methodology and criteria for evaluating technical competencies across DeepShield Systems, Inc. ("Company") engineering, development, and security operations teams.

2. This Framework applies to all technical positions within the Company's Industrial Control System (ICS) security, Operational Technology (OT) protection, and maritime cybersecurity divisions.

2. DEFINITIONS

1. "Technical Competency" refers to measurable skills, knowledge, and capabilities required for specific technical roles within the Company.

2. "Core Technologies" includes the Company's proprietary deep-layer security architecture, SCADA protection systems, and maritime infrastructure security platforms.

3. "Assessment Period" means the quarterly evaluation cycle during which technical skills assessments are conducted.

3. TECHNICAL COMPETENCY DOMAINS

1. Industrial Control Systems Security

- ICS protocol expertise (Modbus, DNP3, OPC-UA)
- SCADA system architecture and security
- PLC programming and security hardening
- Industrial network segmentation

2. Maritime and Subsea Infrastructure

- Maritime control systems security

- Subsea communication protocols
- Offshore platform security architecture
- Maritime IoT security

3. Artificial Intelligence and Analytics
- Machine learning for threat detection
- Behavioral analytics
- Anomaly detection algorithms
- AI model development and validation

4. ASSESSMENT METHODOLOGY

1. Evaluation Components

a) Technical knowledge assessment (40%)

b) Practical skills demonstration (35%)

c) Project portfolio review (15%)

d) Peer assessment (10%)

2. Scoring System
- Level 1: Basic Proficiency (70-79%)
- Level 2: Advanced Implementation (80-89%)
- Level 3: Expert/Architecture (90-100%)

5. ROLE-SPECIFIC REQUIREMENTS

1. Security Engineers
- Minimum Level 2 proficiency in ICS security
- Level 2 proficiency in at least one maritime security domain
- Level 1 proficiency in AI/ML fundamentals

2. Development Team
- Level 2 proficiency in secure coding practices
- Level 2 proficiency in relevant programming languages
- Level 1 proficiency in ICS protocols

3. Architecture Team

- Level 3 proficiency in system architecture
- Level 2 proficiency in maritime security
- Level 2 proficiency in AI/ML implementation

6. ASSESSMENT PROCEDURES

1. Assessment Schedule

- Quarterly technical evaluations
- Annual comprehensive review
- Ad-hoc assessments for project-specific requirements

2. Documentation Requirements

- Detailed assessment results
- Skills gap analysis
- Development recommendations
- Certification status

7. CERTIFICATION AND TRAINING

1. Required Certifications

- Industrial Control Systems Security Professional (ICSP)
- Maritime Cybersecurity Specialist (MCS)
- DeepShield Platform Architect Certification

2. Continuing Education

- Minimum 40 hours annual technical training
- Quarterly internal knowledge sharing sessions
- Industry conference participation

8. COMPLIANCE AND REVIEW

1. This Framework shall be reviewed annually by the Chief Technology Officer and VP of Engineering.

2. Updates to this Framework must be approved by:

- Chief Technology Officer
- VP of Engineering
- Chief Security Architect
- Human Resources Director

9. CONFIDENTIALITY

1. This Framework and all assessment results are confidential and proprietary to DeepShield Systems, Inc.

2. Distribution of this document is restricted to authorized personnel only.

10. EXECUTION

IN WITNESS WHEREOF, this Technical Skills Assessment Framework has been approved and adopted by the undersigned authorized representatives of DeepShield Systems, Inc.

DEEPSHIELD SYSTEMS, INC.

Sarah Blackwood
Chief Technology Officer

James Morrison
VP of Engineering

Dr. Elena Rodriguez
Chief Security Architect

Date: January 15, 2024