ACCESS CONTROL MATRIX - PRODUCTION ENVIRONMENT

DeepShield Systems, Inc.

Document Classification: CONFIDENTIAL

Last Updated: January 11, 2024

Document ID: ACM-PROD-2024-01

1. DOCUMENT PURPOSE AND SCOPE

1. This Access Control Matrix ("ACM") defines the authorized access levels, permissions, and security controls for DeepShield Systems, Inc.'s ("Company") production environment, including all operational technology (OT) infrastructure, industrial control systems (ICS), and related cybersecurity platforms.

2. This document governs access management for all production systems supporting the DeepShield(TM) Industrial Security Platform and associated maritime/subsea protection modules.

2. ACCESS LEVEL DEFINITIONS

1. **Level 0 - No Access**
   - External parties and non-authorized personnel
   - No system access or visibility

2. **Level 1 - Read Only**
   - Security analysts (Tier 1)
   - System monitoring personnel
   - Access limited to viewing system status and logs

3. **Level 2 - Standard Operations**
   - Security analysts (Tier 2)
   - Operations engineers
   - Incident response team members
   - Ability to execute predefined operational procedures

4. **Level 3 - Advanced Operations**
   - Senior security engineers

- Lead operations engineers
- System architects
- Configuration management capabilities
- Incident response coordination

5. **Level 4 - Administrative**
- Security architecture team
- Principal engineers
- Department heads
- Full system administration rights
- Change management authority

6. **Level 5 - Root Access**
- Chief Security Architect
- VP of Engineering
- CTO
- Emergency override capabilities
- System-wide configuration authority

3. SYSTEM COMPONENTS AND ACCESS PERMISSIONS

1. **Core Platform Infrastructure**

Component	L1	L2	L3	L4	L5
Network Monitoring	R	RW	RWX	RWXC	RWXC
Threat Detection	R	RW	RWX	RWXC	RWXC
Response Automation	-	RW	RWX	RWXC	RWXC
Configuration DB	-	R	RW	RWXC	RWXC

2. **Maritime Security Module**

Component	L1	L2	L3	L4	L5
Subsea Sensors	R	RW	RWX	RWXC	RWXC

| Maritime IDS | R | RW | RWX | RWXC | RWXC |

| Fleet Management | - | R | RWX | RWXC | RWXC |

4. ACCESS CONTROL PROCEDURES

1. **Access Request Process**

- All access requests must be submitted via the Access Management Portal
- Requests require manager approval and security team review
- Emergency access procedures detailed in Section 4.4

2. **Authentication Requirements**

- Multi-factor authentication mandatory for all access levels
- Biometric verification required for Level 4 and 5 access
- Session timeout after 30 minutes of inactivity
- Password rotation every 60 days

3. **Access Review and Audit**

- Quarterly review of all active access permissions
- Monthly audit of Level 4 and 5 access activities
- Automated logging of all system access events
- Regular penetration testing of access controls

4. **Emergency Access Procedures**

- Break-glass protocol for emergency root access
- Minimum two authorized Level 5 users required
- Automatic notification to security team
- Full audit trail of emergency access events

5. COMPLIANCE AND ENFORCEMENT

1. This Access Control Matrix is mandatory for all production environment access.

2. Violations of access control policies may result in immediate access revocation and disciplinary action.

3. All access must comply with relevant regulatory requirements including NIST 800-53, IEC 62443,

and NERC CIP standards.

6. DOCUMENT CONTROL

1. **Review and Updates**

- Annual review required
- Updates require Security Council approval
- Version control maintained in Document Management System

2. **Distribution**

- Available to authorized personnel via secure document portal
- External distribution prohibited without written authorization

7. APPROVAL AND AUTHORIZATION

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 11, 2024

James Morrison

VP of Engineering

Date: January 11, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 11, 2024

End of Document