ACCESS CONTROL MATRIX FOR CRITICAL SYSTEMS

DeepShield Systems, Inc.

Document Version: 2.4

Effective Date: January 15, 2024

Document Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This Access Control Matrix ("Matrix") establishes the authorized access levels and permissions for DeepShield Systems, Inc.'s ("Company") critical systems, including Industrial Control System (ICS) security platforms, Operational Technology (OT) environments, and related infrastructure components.

2. This Matrix applies to all employees, contractors, consultants, temporary workers, and other personnel who require access to the Company's critical systems and protected environments.

2. DEFINITIONS

1. "Critical Systems" means the Company's core technology infrastructure, including but not limited to:

a) DeepShield Platform Infrastructure

b) Client-facing Security Operations Centers (SOCs)

c) Development and Testing Environments

d) Production Systems

e) Backup and Recovery Systems

f) SCADA Network Monitoring Systems

2. "Access Levels" are defined as:

- Level 0: No Access
- Level 1: Read-Only
- Level 2: Standard User
- Level 3: Power User
- Level 4: Administrator
- Level 5: System Administrator

- Level 6: Security Administrator

3. ACCESS CONTROL ASSIGNMENTS

1. Executive Leadership

- CEO: Level 4 access to executive dashboards and reporting systems
- CTO: Level 6 access to all technical systems
- CFO: Level 4 access to financial and operational systems
- VP of Engineering: Level 6 access to development and production environments

2. Engineering Team

- Senior Engineers: Level 5 access to assigned systems
- Development Engineers: Level 4 access to development environments
- QA Engineers: Level 3 access to testing environments
- Junior Engineers: Level 2 access to development environments

3. Security Operations

- Chief Security Architect: Level 6 access to all security systems
- Security Analysts: Level 4 access to monitoring systems
- SOC Operators: Level 3 access to incident response systems
- Security Researchers: Level 3 access to testing environments

4. AUTHENTICATION AND AUTHORIZATION REQUIREMENTS

1. Multi-Factor Authentication (MFA)

- Mandatory for all access levels 3 and above
- Biometric verification required for level 6 access
- Hardware security keys required for production system access

2. Access Review and Certification

- Quarterly review of all level 4+ access permissions
- Semi-annual review of all other access levels
- Annual certification of access requirements by department heads

5. SPECIAL ACCESS PROVISIONS

1. Emergency Access Protocol

- Break-glass procedures for critical system access
- Temporary elevation of privileges during incidents
- Automated logging and notification of emergency access

2. Third-Party Access

- Vendor access limited to Level 2 unless specifically authorized
- Contractor access requires executive approval
- Partner integration access governed by separate agreements

6. COMPLIANCE AND AUDIT

1. Access Logging Requirements

- All system access attempts must be logged
- Access logs retained for minimum of 365 days
- Real-time alerting for unauthorized access attempts

2. Audit Procedures

- Monthly access pattern analysis
- Quarterly privilege usage review
- Annual comprehensive access audit

7. ENFORCEMENT AND VIOLATIONS

1. Any violation of this Matrix may result in:

- Immediate access suspension
- Security incident investigation
- Disciplinary action up to termination
- Legal action where applicable

8. MODIFICATIONS AND UPDATES

1. This Matrix shall be reviewed and updated:

- Annually at minimum
- Upon significant organizational changes

- Following major security incidents
- As required by regulatory changes

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by the undersigned authorized representatives of DeepShield Systems, Inc.

Date: January 15, 2024

Dr. Marcus Chen
Chief Executive Officer

Sarah Blackwood
Chief Technology Officer

Dr. Elena Rodriguez
Chief Security Architect

DOCUMENT CONTROL

Version: 2.4
Last Updated: January 15, 2024
Next Review Date: January 15, 2025
Document Owner: Security Operations
Classification: CONFIDENTIAL