ACCESS CONTROL POLICY AND PROCEDURES

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document ID: POL-SEC-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Access Control Policy and Procedures document ("Policy") establishes the requirements and procedures for managing access to DeepShield Systems, Inc.'s ("Company") information systems, operational technology (OT) environments, and critical infrastructure protection platforms.

2. This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel granted access to Company systems, including but not limited to the DeepShield Platform, SCADA monitoring systems, and industrial control system (ICS) security infrastructure.

2. DEFINITIONS

1. "Access Control" means the selective restriction of access to Company resources.

2. "Privileged Access" refers to elevated system permissions that provide capability to alter system configurations, access critical infrastructure controls, or modify security parameters.

3. "Multi-Factor Authentication (MFA)" means authentication using two or more factors: something you know, something you have, or something you are.

4. "Zero Trust Architecture" refers to security concept requiring strict identity verification for every person and device attempting to access resources.

3. ACCESS CONTROL PRINCIPLES

1. Least Privilege

- Access rights shall be granted based on the principle of least privilege
- Users shall receive minimum access levels required for their role
- Access rights shall be reviewed quarterly

2. Separation of Duties

- Critical operations shall require multiple authorized personnel
- Development and production environments shall maintain strict separation
- System administration and security audit functions shall be segregated

3. Need-to-Know

- Access to client data, proprietary algorithms, and security configurations shall be restricted to personnel with documented business need
- Access justification shall be recorded and maintained

4. ACCESS AUTHORIZATION PROCEDURES

1. Request Process

- Access requests must be submitted through the Company's Identity and Access Management (IAM) system
- Requests must include business justification and manager approval
- Emergency access procedures require CISO or designee approval

2. Approval Requirements

- Standard access requires department manager approval
- Privileged access requires additional approval from Security Operations
- Client environment access requires client authorization and compliance verification

3. Documentation

- All access grants shall be documented in the IAM system
- Approval chain and justification shall be maintained for audit purposes
- Access review logs shall be retained for minimum 3 years

5. AUTHENTICATION REQUIREMENTS

1. All system access shall require:

- Minimum 16-character complex passwords
- Multi-factor authentication
- Biometric verification for privileged access
- 90-day password rotation
- Password history enforcement (12 generations)

2. Failed Authentication

- Accounts shall lock after 3 failed attempts
- Unlock requires Security Operations intervention
- All failed attempts shall be logged and analyzed

6. MONITORING AND AUDIT

1. Continuous Monitoring

- Access patterns shall be monitored in real-time
- Anomaly detection systems shall flag suspicious activity
- Automated alerts shall be generated for policy violations

2. Periodic Reviews

- Access rights shall be reviewed quarterly
- Privileged accounts shall be reviewed monthly
- Inactive accounts shall be disabled after 30 days
- Terminated user access shall be removed within 24 hours

7. COMPLIANCE AND ENFORCEMENT

1. Policy violations may result in:

- Immediate access revocation
- Disciplinary action up to termination
- Legal action where applicable

2. Compliance Requirements

- Annual security awareness training
- Quarterly compliance attestation
- Regular policy acknowledgment

8. POLICY MAINTENANCE

1. This Policy shall be reviewed annually and updated as needed to reflect:

- Changes in technology infrastructure
- New security threats and countermeasures

- Regulatory requirements
- Operational needs

9. EXCEPTIONS

1. Policy exceptions require:

- Written business justification
- CISO approval
- Documentation in risk register
- Quarterly review

APPROVAL AND REVISION HISTORY

Version 2.0 Approved by:

_

Dr. Marcus Chen

Chief Executive Officer

_

Sarah Blackwood

Chief Technology Officer

_

Dr. Elena Rodriguez

Chief Security Architect

Date: January 1, 2024