Physical Access Control Policy - Secure Facilities

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: SEC-PAC-2024-01

Version: 2.1

1. Purpose and Scope

1. This Physical Access Control Policy ("Policy") establishes the requirements and procedures for physical access control at DeepShield Systems, Inc. ("Company") secure facilities, including research and development centers, data centers, and critical infrastructure testing environments.

2. This Policy applies to all employees, contractors, visitors, and third-party service providers requiring access to Company secure facilities.

2. Definitions

1. "Secure Facilities" means Company locations designated as containing sensitive equipment, data, or operations, including:

a) Research & Development Labs

b) Network Operations Centers

c) Data Centers

d) Industrial Control System Testing Environments

e) Maritime Security Simulation Facilities

2. "Access Credentials" means any physical or electronic means of authentication, including:

a) Security badges

b) Biometric identifiers

c) PIN codes

d) Electronic key cards

e) Physical keys

3. Access Authorization Levels

1. Level 1 - General Access

- Basic building access during business hours
- Access to common areas and non-restricted zones
- Requires standard employee badge

2. Level 2 - Restricted Access

- Access to R&D areas and testing laboratories
- Extended hours access
- Requires enhanced verification and management approval

3. Level 3 - Critical Access

- Access to high-security areas (data centers, NOC)
- 24/7 access capabilities
- Requires executive approval and background check
- Dual authentication required

4. Access Authorization Procedures

1. Access Request Process

a) Submission of formal access request through Security Portal

b) Manager approval documentation

c) Security background check completion

d) Completion of required security training

e) Signed confidentiality agreement

2. Temporary Access

a) Maximum duration of 30 days

b) Sponsor required (Level 2 or higher)

c) Daily sign-in/sign-out procedure

d) Escort required for Level 2 and 3 areas

5. Security Controls and Monitoring

1. Physical Security Measures

- 24/7 security personnel

- CCTV surveillance systems
- Multi-factor authentication at entry points
- Man-trap entries for Level 3 areas
- Biometric verification systems

2. Access Monitoring

- Real-time access logging
- Video recording retention (90 days minimum)
- Regular access pattern analysis
- Automated anomaly detection
- Monthly access audit reports

6. Emergency Procedures

1. Emergency Access Protocol

- Emergency override procedures for first responders
- Designated emergency coordinators
- Backup access systems
- Emergency evacuation routes and procedures

2. Security Breach Response

- Immediate access suspension capabilities
- Incident response team activation
- Forensic investigation procedures
- Regulatory notification requirements

7. Compliance and Enforcement

1. Policy Violations

- Immediate access suspension
- Disciplinary action up to termination
- Potential legal action for serious breaches
- Incident reporting to relevant authorities

2. Audit Requirements

- Quarterly access review
- Annual policy compliance audit
- Third-party security assessment
- Regulatory compliance verification

8. Policy Administration

1. Review and Updates

- Annual policy review
- Quarterly security assessment
- Update based on incident learnings
- Regulatory requirement monitoring

2. Documentation Requirements

- Access request records (7 years)
- Incident reports (5 years)
- Training records (3 years)
- Audit logs (2 years)

9. Approval and Implementation

This Policy is approved and implemented by:

/s/ Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 15, 2024

10. Document Control

Version History:

- 2.1: January 15, 2024 - Updated emergency procedures
- 2.0: July 1, 2023 - Major revision
- 1.0: March 15, 2022 - Initial release

Distribution: CONFIDENTIAL - Internal Use Only

Security Classification: Level 2 - Restricted