PHYSICAL SECURITY DESIGN REQUIREMENTS

DeepShield Systems, Inc.

Document No. SEC-PDR-2024-001

Effective Date: January 15, 2024

Version 3.2

1. PURPOSE AND SCOPE

1. This document establishes the minimum physical security design requirements for all DeepShield Systems, Inc. ("Company") facilities, including corporate offices, research and development centers, and customer deployment sites where Company personnel maintain a permanent presence.

2. These requirements apply to:

a) New facility construction

b) Facility renovations

c) Security system upgrades

d) Temporary secure areas

e) Remote monitoring stations

2. FACILITY CLASSIFICATION

1. All Company facilities shall be classified according to the following security levels:

Level 1: Public Access Areas

Level 2: General Office Areas

Level 3: Restricted Operations Areas

Level 4: Critical Security Areas

Level 5: High-Security Development Zones

2. Each security level requires progressively more stringent security controls as detailed in Sections 3-7.

3. PERIMETER SECURITY REQUIREMENTS

1. Physical Barriers

a) Minimum 8-foot perimeter fencing for Level 3-5 facilities

b) Anti-climb features on all security fencing

c) Vehicle barriers at all vehicle entry points

d) Reinforced concrete bollards protecting building approaches

2. Entry Points

a) Limited to the minimum necessary for operations

b) Mantrap configurations for Level 4-5 areas

c) Anti-tailgating measures

d) Emergency egress compliance with NFPA 101

4. ACCESS CONTROL SYSTEMS

1. Authentication Methods

a) Minimum dual-factor authentication for Level 3+

b) Biometric verification for Level 4-5

c) PIN codes minimum 6 digits

d) Smart card specifications per ISO/IEC 14443

2. System Requirements

a) UL 294 Listed components

b) Encrypted communication protocols

c) Backup power for 24-hour operation

d) Real-time monitoring capability

5. SURVEILLANCE SYSTEMS

1. Camera Coverage

a) 100% coverage of Level 3-5 areas

b) 90-day minimum recording retention

c) Minimum 1080p resolution

d) Low-light capability

2. Monitoring Requirements

a) 24/7 monitoring for Level 4-5 areas

b) Motion detection analytics

c) Automated alert system

d) Backup recording systems

6. SECURE DEVELOPMENT ENVIRONMENTS

1. Level 5 Area Requirements

a) RF shielding to TEMPEST standards

b) White noise systems

c) Anti-surveillance countermeasures

d) Faraday cage construction

2. Environmental Controls

a) Independent HVAC systems

b) EMI shielding

c) Acoustic isolation

d) EMP protection measures

7. COMPLIANCE AND AUDIT

1. Documentation Requirements

a) As-built drawings

b) System configurations

c) Maintenance records

d) Incident reports

2. Audit Schedule

a) Quarterly physical security assessments

b) Annual third-party audits

c) Monthly system testing

d) Daily equipment checks

8. IMPLEMENTATION AND MAINTENANCE

1. All security systems must be installed by Company-approved contractors holding appropriate certifications.

2. Maintenance schedules shall follow manufacturer specifications and Company standards, whichever is more stringent.

9. EXCEPTIONS AND DEVIATIONS

1. Exceptions to these requirements must be approved in writing by:

a) Chief Security Architect

b) VP of Engineering

c) Chief Technology Officer

10. DOCUMENT CONTROL

1. This document shall be reviewed annually and updated as required.

2. Distribution limited to authorized personnel with Level 3 or higher clearance.

APPROVAL AND AUTHORIZATION

APPROVED BY:

Dr. Elena Rodriguez

Chief Security Architect

Date: _

James Morrison

VP of Engineering

Date: _

Sarah Blackwood

Chief Technology Officer

Date: _