SECURITY CLEARANCE REQUIREMENTS BY ROLE

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: CONFIDENTIAL

1. PURPOSE AND SCOPE

1. This document establishes the mandatory security clearance requirements for all employees, contractors, and consultants ("Personnel") of DeepShield Systems, Inc. ("Company") based on their roles and access levels to sensitive information, critical infrastructure systems, and proprietary technology.

2. These requirements are established pursuant to federal regulations, contractual obligations with government agencies and critical infrastructure clients, and Company security policies.

2. DEFINITIONS

1. "Security Clearance" refers to an authorization that allows access to classified information or restricted areas, granted after completion of a background investigation.

2. "Critical Role" means any position that requires access to Level 1 or Level 2 systems as defined in the Company's System Access Matrix.

3. "Sensitive Information" includes but is not limited to: proprietary technology specifications, client infrastructure data, security vulnerability assessments, and classified government contract information.

3. CLEARANCE LEVELS BY ROLE CATEGORY

3.1. Executive Leadership

- CEO, CTO, CFO: Top Secret/SCI clearance required
- VP-level executives: Secret clearance minimum
- Regional Directors: Secret clearance minimum

3.2. Engineering and Development

- Chief Security Architect: Top Secret/SCI clearance required
- Senior Security Engineers: Secret clearance required
- Development Team Leads: Secret clearance required
- Software Engineers: Confidential clearance minimum
- QA Engineers: Confidential clearance minimum

3.3. Operations and Support

- Security Operations Center (SOC) Manager: Secret clearance required
- SOC Analysts: Secret clearance required
- Technical Support Engineers: Confidential clearance minimum
- Customer Success Managers: Confidential clearance minimum

3.4. Sales and Business Development

- Federal Sales Team: Secret clearance required
- Commercial Sales Team: Company background check required
- Business Development Directors: Secret clearance required
- Solution Architects: Secret clearance required

4. CLEARANCE ACQUISITION AND MAINTENANCE

1. The Company shall sponsor security clearance applications for eligible Personnel as required by their role.

2. Personnel must:

a) Submit to required background investigations

b) Complete security awareness training annually

c) Report any changes that may affect clearance status

d) Maintain continuous compliance with clearance requirements

3. Interim Access Provisions:

a) Temporary access may be granted pending clearance approval

b) Must be approved by Security Director and Department VP

c) Limited to 180 days maximum

d) Subject to enhanced monitoring and restrictions

5. COMPLIANCE AND ENFORCEMENT

1. The Security Compliance Office shall:

a) Maintain records of all clearance statuses

b) Monitor compliance with renewal requirements

c) Conduct quarterly audits of access controls

d) Report violations to Executive Leadership

2. Non-compliance may result in:

a) Immediate access restriction

b) Disciplinary action up to termination

c) Legal action for security violations

d) Reporting to relevant authorities

6. SPECIAL PROJECT REQUIREMENTS

1. Maritime Security Projects:

a) Additional TWIC card requirement

b) Port security clearance as applicable

c) International maritime security certifications

2. Government Contracts:

a) Additional agency-specific clearances

b) Special Access Program (SAP) clearances

c) Facility Security Clearance requirements

7. CONFIDENTIALITY AND NON-DISCLOSURE

1. All information regarding security clearance status, processes, and requirements is classified as Confidential.

2. Personnel shall not disclose clearance information except as required by law or authorized by Security Director.

8. AMENDMENTS AND UPDATES

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

2. Changes require approval from:

a) Chief Security Officer

b) General Counsel

c) Board of Directors for substantial changes

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by the Board of Directors of DeepShield Systems, Inc.

Date: January 15, 2024

_

Dr. Marcus Chen

Chief Executive Officer

_

Sarah Blackwood

Chief Technology Officer

_

Robert Kessler

Chief Financial Officer

WITNESSED:

_

Corporate Secretary