ASSET MANAGEMENT SECURITY STANDARDS

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: Confidential

1. PURPOSE AND SCOPE

1. This Asset Management Security Standards document ("Standards") establishes the mandatory requirements and procedures for securing, managing, and protecting DeepShield Systems, Inc.'s ("Company") critical assets, including operational technology (OT) infrastructure, industrial control systems (ICS), and related intellectual property.

2. These Standards apply to all Company employees, contractors, consultants, temporary workers, and other business partners who access, manage, or maintain Company assets.

2. DEFINITIONS

1. "Critical Assets" means any Company-owned or managed hardware, software, data, or intellectual property essential to the Company's operations, including:

a) Industrial Control System (ICS) components

b) SCADA network infrastructure

c) Proprietary security algorithms and models

d) Customer deployment configurations

e) AI/ML training datasets

f) Source code repositories

2. "Asset Classification Levels" shall be designated as follows:

- Level 1: Mission Critical
- Level 2: Business Critical
- Level 3: Operational
- Level 4: General Purpose

3. ASSET INVENTORY AND CLASSIFICATION

1. The Company shall maintain a comprehensive asset inventory system that:

a) Uniquely identifies and tracks all Critical Assets

b) Documents asset ownership and responsible parties

c) Records asset classification levels

d) Maintains chain of custody records

e) Tracks asset location and deployment status

2. Assets must be classified according to:

a) Business impact

b) Security requirements

c) Regulatory compliance obligations

d) Customer contractual requirements

4. SECURITY CONTROLS

1. Physical Security Controls

a) All Critical Assets must be stored in access-controlled facilities

b) Biometric authentication required for Level 1 and 2 assets

c) Video surveillance coverage of asset storage areas

d) Environmental monitoring systems

e) Redundant power systems

2. Technical Security Controls

a) Encryption of all data at rest and in transit

b) Multi-factor authentication for asset access

c) Automated vulnerability scanning

d) Real-time security monitoring

e) Secure backup systems

f) Access logging and audit trails

5. ACCESS MANAGEMENT

1. Access to Critical Assets shall be:

a) Granted on a need-to-know basis

b) Reviewed quarterly

c) Documented in the access management system

d) Revoked immediately upon termination

e) Subject to periodic compliance audits

2. Privileged Access Requirements:

a) Enhanced authentication controls

b) Time-limited access windows

c) Supervised access for Level 1 assets

d) Activity logging and review

e) Quarterly access recertification

6. INCIDENT RESPONSE

1. Security incidents involving Critical Assets must be:

a) Reported immediately to the Security Operations Center

b) Documented in the incident management system

c) Investigated according to severity level

d) Remediated following approved procedures

e) Reviewed for lessons learned

2. Incident Classification Matrix:

- Severity 1: Asset compromise or loss
- Severity 2: Unauthorized access attempt
- Severity 3: Policy violation
- Severity 4: Suspicious activity

7. COMPLIANCE AND AUDIT

1. Regular Audits

a) Quarterly internal security audits

b) Annual third-party compliance assessments

c) Continuous automated compliance monitoring

d) Regular penetration testing

e) Asset inventory reconciliation

2. Documentation Requirements

a) Asset management procedures

b) Security control implementations

c) Access authorization records

d) Incident response reports

e) Audit findings and remediation

8. ENFORCEMENT

1. Violations of these Standards may result in:

a) Disciplinary action up to termination

b) Legal action where applicable

c) Revocation of access privileges

d) Mandatory security training

e) Enhanced monitoring

9. REVIEW AND UPDATES

1. These Standards shall be:

a) Reviewed annually

b) Updated as required by threat landscape

c) Approved by the Chief Security Architect

d) Distributed to all affected parties

e) Version controlled and archived

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, the undersigned has executed these Standards as of the Effective Date.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

Date: January 15, 2024