CRITICAL ASSET INVENTORY MANAGEMENT PROTOCOL

DEEPSHIELD SYSTEMS, INC.

Effective Date: January 15, 2024

Document ID: DSS-CAIMP-2024-01

Version: 2.0

1. PURPOSE AND SCOPE

1. This Critical Asset Inventory Management Protocol ("Protocol") establishes mandatory procedures for identifying, cataloging, and managing critical assets within DeepShield Systems, Inc.'s ("Company") operational technology (OT) security infrastructure and client deployment environments.

2. This Protocol applies to all Company employees, contractors, and authorized third parties involved in the deployment, maintenance, or monitoring of the Company's industrial control system (ICS) security solutions.

2. DEFINITIONS

1. "Critical Assets" means any hardware, software, data, or infrastructure components essential to:

(a) The Company's proprietary deep-layer security architecture;

(b) Client SCADA networks and industrial automation systems;

(c) Maritime and subsea infrastructure protection systems;

(d) AI-driven threat detection and response mechanisms.

2. "Asset Registry" means the Company's secure digital repository containing detailed records of all Critical Assets.

3. "Security Classification Levels" means the tiered system (Level 1-4) used to categorize Critical Assets based on operational importance and security sensitivity.

3. ASSET IDENTIFICATION AND CLASSIFICATION

1. All Critical Assets must be identified and classified according to the following criteria:

(a) Operational significance

(b) Security sensitivity

(c) Regulatory compliance requirements

(d) Business continuity impact

(e) Replacement/recovery timeframes

2. Security Classification Levels shall be assigned as follows:

- Level 1: Mission-critical components of deep-layer security architecture
- Level 2: Primary client-facing security systems
- Level 3: Supporting infrastructure and backup systems
- Level 4: Auxiliary components and non-critical assets

4. INVENTORY MANAGEMENT REQUIREMENTS

1. Asset Registry Maintenance

(a) The Asset Registry must be updated within 24 hours of any Critical Asset:

- Deployment
- Modification
- Decommissioning
- Transfer

(b) Each Registry entry must include:

- Unique asset identifier
- Security Classification Level
- Physical/virtual location
- Responsible personnel
- Maintenance history
- Security clearance requirements

2. Periodic Auditing

(a) Level 1 assets: Monthly audit

(b) Level 2 assets: Quarterly audit

(c) Level 3 assets: Semi-annual audit

(d) Level 4 assets: Annual audit

5. ACCESS CONTROL AND SECURITY MEASURES

1. Access to Critical Assets shall be restricted based on:

(a) Security Classification Level

(b) Job function necessity

(c) Security clearance status

(d) Training certification completion

2. Documentation Requirements

(a) All access to Level 1 and 2 assets must be logged

(b) Access logs must be retained for minimum 3 years

(c) Quarterly access review by Security Operations

6. COMPLIANCE AND REPORTING

1. The Chief Security Architect shall:

(a) Maintain compliance with this Protocol

(b) Generate monthly compliance reports

(c) Review Protocol effectiveness quarterly

(d) Recommend Protocol updates as needed

2. Non-Compliance

(a) Violations must be reported within 24 hours

(b) Investigation required within 48 hours

(c) Remediation plan required within 72 hours

7. PROTOCOL REVIEW AND UPDATES

1. This Protocol shall be reviewed annually by:

(a) Chief Security Architect

(b) VP of Engineering

(c) Chief Technology Officer

(d) General Counsel

2. Emergency updates may be implemented with CEO approval

8. CONFIDENTIALITY

1. This Protocol and all related documentation are classified as Confidential Information under the Company's Information Security Policy.

9. AUTHORIZATION

This Protocol is hereby authorized and adopted by:

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Marcus Chen

Chief Executive Officer

Date:

By:

Dr. Elena Rodriguez

Chief Security Architect

Date:

10. REVISION HISTORY

Version 2.0 - January 15, 2024

Version 1.1 - March 20, 2023

Version 1.0 - June 15, 2022