ASSET CLASSIFICATION GUIDELINES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: DSS-SEC-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. This Asset Classification Guidelines document ("Guidelines") establishes the framework for identifying, categorizing, and protecting information assets and operational technology (OT) resources within DeepShield Systems, Inc. ("Company").

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

2. DEFINITIONS

1. "Assets" means all information, data, systems, networks, equipment, facilities, and resources owned, controlled, or operated by the Company.

2. "Critical Infrastructure Assets" means OT systems, industrial control systems (ICS), SCADA networks, and related components that support essential operations.

3. "Intellectual Property Assets" means proprietary algorithms, source code, technical documentation, and research related to the Company's deep-layer security architecture.

3. ASSET CLASSIFICATION LEVELS

1. **Level 1 - Restricted**

- Critical infrastructure protection algorithms
- Customer security configurations
- Authentication protocols and encryption keys
- Source code for core security modules
- Maritime defense system specifications

2. **Level 2 - Confidential**

- Network topology diagrams
- System architecture documentation
- Customer implementation guides
- Threat detection models
- Internal security policies

3. **Level 3 - Internal Use**

- Training materials
- Operating procedures
- Product documentation
- Technical specifications
- Project plans

4. **Level 4 - Public**

- Marketing materials
- Public product descriptions
- Published research papers
- Press releases
- General company information

4. CLASSIFICATION CRITERIA

1. Assets shall be classified based on:

- Criticality to business operations
- Regulatory compliance requirements
- Potential impact of unauthorized disclosure
- Customer contractual obligations
- Intellectual property value

2. Classification assessment must consider:

- Asset type and purpose
- Legal and regulatory context
- Security requirements

- Access control needs
- Data retention requirements

5. HANDLING REQUIREMENTS

1. **Restricted Assets**

- Encryption required for storage and transmission
- Multi-factor authentication mandatory
- Access limited to named individuals
- Audit logging of all access events
- Quarterly access review required

2. **Confidential Assets**

- Encryption required for external transmission
- Role-based access control
- Department-level authorization required
- Access logging mandatory
- Semi-annual access review

3. **Internal Use Assets**

- Standard access controls
- Employee authentication required
- Department-level access permitted
- Basic activity logging
- Annual access review

6. RESPONSIBILITIES

1. **Asset Owners**

- Determine initial classification level
- Review classification periodically
- Authorize access requests
- Ensure compliance with handling requirements

2. **Information Security Team**

- Maintain classification guidelines
- Provide implementation guidance
- Conduct compliance audits
- Review classification decisions

3. **Employees**

- Understand classification levels
- Follow handling requirements
- Report security incidents
- Protect assigned assets

7. COMPLIANCE AND ENFORCEMENT

1. Compliance with these Guidelines is mandatory for all personnel.

2. Violations may result in disciplinary action up to and including termination.

3. Regular audits will be conducted to ensure compliance.

8. REVIEW AND UPDATES

1. These Guidelines shall be reviewed annually by the Information Security Team.

2. Updates require approval from the Chief Security Architect and Chief Technology Officer.

9. LEGAL NOTICE

These Guidelines are confidential and proprietary to DeepShield Systems, Inc. Unauthorized disclosure, copying, or distribution is prohibited. This document is protected under applicable intellectual property laws.

Approved by:

Dr. Elena Rodriguez

Chief Security Architect

Date: January 15, 2024

Sarah Blackwood

Chief Technology Officer

Date: January 15, 2024