CLOUD SECURITY ARCHITECTURE STANDARDS

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document Version: 3.2

Classification: Confidential

1. INTRODUCTION

1. This Cloud Security Architecture Standards document ("Standards") establishes the mandatory security requirements and architectural principles for all cloud-based components of DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security solutions and operational technology (OT) protection platforms.

2. These Standards apply to all cloud infrastructure, platforms, and services utilized in the delivery of the Company's proprietary deep-layer security architecture and related services.

2. DEFINITIONS

1. "Cloud Services" means any Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) components utilized by the Company.

2. "Critical Infrastructure" means the physical and virtual systems and assets vital to the Company's operations and customer deployments.

3. "Security Architecture" means the structured security controls, protocols, and design principles implemented across the Company's cloud environment.

3. ARCHITECTURAL PRINCIPLES

1. Zero Trust Architecture

- All network traffic must be authenticated and encrypted
- Implementation of micro-segmentation for all cloud workloads
- Continuous validation of security posture and compliance
- Just-in-time access control for all administrative functions

2. Defense in Depth

- Multiple layers of security controls across all cloud services
- Redundant security mechanisms for critical systems
- Separation of duties between production and development environments
- Automated security testing and validation procedures

4. SECURITY REQUIREMENTS

1. Identity and Access Management

- Multi-factor authentication required for all administrative access
- Role-based access control (RBAC) implementation
- Regular access reviews and privilege attestation
- Automated deprovisioning of unused accounts

2. Data Protection

- Encryption at rest using AES-256 for all stored data
- TLS 1.3 required for all data in transit
- Regular key rotation and cryptographic hygiene
- Secure key management system implementation

3. Network Security

- Virtual private cloud (VPC) isolation for customer environments
- Web application firewall (WAF) implementation
- DDoS protection and mitigation controls
- Network segmentation and microsegmentation

5. COMPLIANCE AND MONITORING

1. Continuous Monitoring

- Real-time security event monitoring and alerting
- Automated vulnerability scanning and assessment
- Performance monitoring and metrics collection
- Security information and event management (SIEM) integration

2. Compliance Requirements

- Regular compliance assessments against ISO 27001
- SOC 2 Type II controls maintenance
- Industry-specific compliance validation
- Documentation of all security controls and procedures

6. INCIDENT RESPONSE

1. Incident Management

- Defined incident response procedures and playbooks
- Automated incident detection and response capabilities
- Regular testing of incident response procedures
- Integration with customer notification systems

2. Business Continuity

- Disaster recovery procedures for cloud services
- Regular backup and restoration testing
- Geographic redundancy for critical services
- Recovery time objective (RTO) and recovery point objective (RPO) definitions

7. REVIEW AND UPDATES

1. These Standards shall be reviewed and updated annually or upon significant changes to the Company's cloud infrastructure or security requirements.

2. All updates must be approved by the Chief Security Architect and Chief Technology Officer.

8. ENFORCEMENT

1. Compliance with these Standards is mandatory for all employees, contractors, and third-party service providers accessing or managing Company cloud resources.

2. Violations of these Standards may result in disciplinary action, up to and including termination of employment or service agreements.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED by the undersigned, effective as of the date first written above.

DEEPSHIELD SYSTEMS, INC.

By:

Name: Dr. Elena Rodriguez

Title: Chief Security Architect

By:

Name: Sarah Blackwood

Title: Chief Technology Officer

DOCUMENT CONTROL

Version: 3.2

Last Review Date: December 15, 2023

Next Review Date: December 15, 2024

Document Owner: Security Architecture Team

Classification: Confidential