CHANGE MANAGEMENT SECURITY GUIDELINES

DeepShield Systems, Inc.

Effective Date: January 15, 2024

Document ID: DSS-SEC-2024-001

Version: 2.0

1. PURPOSE AND SCOPE

1. These Change Management Security Guidelines ("Guidelines") establish the mandatory procedures and security controls governing all changes to DeepShield Systems, Inc.'s ("Company") operational technology (OT) environments, industrial control systems (ICS), and related cybersecurity infrastructure.

2. These Guidelines apply to all employees, contractors, consultants, temporary workers, and other personnel who may implement or authorize changes to the Company's critical systems and infrastructure.

2. DEFINITIONS

1. "Change" means any modification, addition, or removal of hardware, software, network configurations, security controls, or operational procedures that may impact the Company's industrial cybersecurity platforms or client environments.

2. "Emergency Change" refers to modifications required to resolve a critical security incident or system failure that poses immediate risk to operations or client security.

3. "Change Advisory Board" or "CAB" means the designated group of technical and business leaders responsible for reviewing and approving proposed changes.

3. CHANGE MANAGEMENT PROCEDURES

1. Standard Change Process

a) All proposed changes must be documented in the Company's Change Management System

b) Changes must include detailed implementation and rollback plans

c) Risk assessments must be completed for all changes

d) Changes affecting client environments require additional security review

e) Testing must be performed in isolated environments before production deployment

2. Emergency Change Process

a) Emergency changes require immediate notification to the Security Operations Center

b) Post-implementation documentation must be completed within 24 hours

c) Emergency changes require retrospective CAB review within 72 hours

4. SECURITY REQUIREMENTS

1. Access Controls

a) Only authorized personnel may implement approved changes

b) Multi-factor authentication required for all system modifications

c) Privileged access credentials must be checked out through PAM system

d) All access must be logged and monitored

2. Security Testing

a) Vulnerability scanning required pre and post-change

b) Security impact analysis mandatory for infrastructure changes

c) Penetration testing required for significant architecture modifications

d) Client notification required for changes affecting security posture

5. DOCUMENTATION AND AUDIT

1. Required Documentation

a) Detailed change description and business justification

b) Technical implementation specifications

c) Security impact assessment

d) Test results and validation procedures

e) Approval chain documentation

f) Client notifications where applicable

2. Audit Requirements

a) All changes must be logged in immutable audit system

b) Quarterly compliance reviews of change management processes

c) Annual third-party audit of security controls

d) Retention of change documentation for minimum 3 years

6. COMPLIANCE AND ENFORCEMENT

1. All personnel must comply with these Guidelines. Violations may result in disciplinary action up to and including termination of employment or service agreement.

2. The Chief Security Architect shall conduct quarterly compliance reviews and report findings to executive management.

7. EXCEPTIONS AND DEVIATIONS

1. Exceptions to these Guidelines must be approved in writing by both:

a) Chief Security Architect or designee

b) VP of Engineering or designee

2. All exceptions must be documented and reviewed quarterly by the CAB.

8. REVIEW AND UPDATES

1. These Guidelines shall be reviewed and updated annually or upon significant changes to:

a) Regulatory requirements

b) Industry security standards

c) Company technology infrastructure

d) Risk assessment findings

9. AUTHORITY AND RESPONSIBILITY

1. The Chief Security Architect is responsible for maintaining and enforcing these Guidelines.

2. The Change Advisory Board has authority to approve or reject all proposed changes.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 15th day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Dr. Elena Rodriguez

Chief Security Architect

By:

James Morrison

VP of Engineering