SECURITY PATCH MANAGEMENT STANDARD OPERATING PROCEDURE

DeepShield Systems, Inc.

Document No.: SOP-SEC-2024-001

Effective Date: January 15, 2024

Version: 2.0

1. PURPOSE AND SCOPE

1. This Standard Operating Procedure ("SOP") establishes the requirements and processes for managing security patches across DeepShield Systems, Inc.'s ("Company") technology infrastructure, including operational technology (OT) environments, industrial control systems (ICS), and corporate information technology (IT) systems.

2. This SOP applies to all Company employees, contractors, and third-party service providers who are responsible for maintaining, updating, or securing Company systems and client-deployed solutions.

2. DEFINITIONS

1. "Critical Patch" means any software update that addresses security vulnerabilities with a CVSS score of 7.0 or higher.

2. "OT Environment" means operational technology systems, including industrial control systems, SCADA networks, and related infrastructure.

3. "Patch Window" means the Company-approved timeframe during which system updates may be implemented.

4. "Testing Environment" means the Company's designated infrastructure for validating patches prior to production deployment.

3. ROLES AND RESPONSIBILITIES

1. Security Operations Team

- Monitor security advisory feeds and vulnerability announcements

- Evaluate patch criticality and deployment priorities
- Maintain patch management documentation

2. OT Systems Engineering

- Review patches for OT environment compatibility
- Coordinate with clients for deployment scheduling
- Execute patch deployment in industrial environments

3. Quality Assurance Team

- Test patches in simulation environment
- Validate system functionality post-patch
- Document testing results and recommendations

4. PATCH MANAGEMENT PROCEDURE

1. Patch Identification and Assessment

a) Security Operations shall monitor vendor security advisories daily

b) Patches shall be categorized by criticality level:

- Critical (CVSS 9.0-10.0): 24-hour response required
- High (CVSS 7.0-8.9): 72-hour response required
- Medium (CVSS 4.0-6.9): 7-day response required
- Low (CVSS 0.1-3.9): Next scheduled maintenance window

2. Testing Requirements

a) All patches must undergo testing in the Testing Environment

b) Testing must include:

- Functionality verification
- Integration testing
- Performance impact assessment
- Rollback procedure validation

3. Deployment Authorization

a) Critical patches require CTO or designee approval

b) High-risk patches require Security Director approval

c) Medium/Low-risk patches require Security Manager approval

5. DEPLOYMENT PROCEDURES

1. Pre-Deployment

a) Create deployment schedule

b) Notify affected stakeholders

c) Verify system backups

d) Document rollback procedures

2. Deployment Execution

a) Implement patches during approved maintenance windows

b) Follow change management procedures

c) Monitor system performance during deployment

d) Document deployment steps and results

3. Post-Deployment

a) Verify system functionality

b) Update patch management database

c) Close associated change tickets

d) Archive deployment documentation

6. EMERGENCY PATCHING

1. Emergency patches may bypass standard procedures when:

a) Active exploitation is detected

b) Regulatory authorities mandate immediate action

c) Critical business operations are at risk

2. Emergency Approval Process

a) Obtain verbal approval from CTO or CEO

b) Document deviation from standard procedures

c) Conduct post-deployment review within 24 hours

7. COMPLIANCE AND REPORTING

1. Maintain detailed records of:

a) Patch deployment history

b) Testing results

c) Approval documentation

d) System exceptions

2. Generate monthly compliance reports including:

a) Patch status across all systems

b) Outstanding vulnerabilities

c) Deployment metrics

d) Exception justifications

8. DOCUMENT CONTROL

1. This SOP shall be reviewed annually by the Security Operations team.

2. Modifications require approval from:

- Chief Technology Officer
- Chief Security Architect
- VP of Engineering

9. SIGNATURE AND APPROVAL

APPROVED BY:

Sarah Blackwood

Chief Technology Officer

Date: _

Dr. Elena Rodriguez

Chief Security Architect

Date: _

James Morrison

VP of Engineering

Date: _