BACKUP AND RECOVERY PROCEDURES - CRITICAL SYSTEMS

DeepShield Systems, Inc.

Effective Date: January 1, 2024

Document ID: DSS-BRP-2024-001

Version: 3.0

1. PURPOSE AND SCOPE

1. This document establishes mandatory procedures for the backup and recovery of critical systems supporting DeepShield Systems, Inc.'s ("Company") industrial control system (ICS) security platform and related operational technology (OT) infrastructure.

2. These procedures apply to all mission-critical systems, including but not limited to:

a) DeepShield Core Platform infrastructure

b) Customer-facing security monitoring systems

c) Threat intelligence databases

d) AI/ML training environments

e) SCADA protection frameworks

f) Maritime defense system components

2. DEFINITIONS

1. "Critical Systems" means any system component whose failure would result in severe degradation of service delivery to customers or pose a risk to protected infrastructure.

2. "Recovery Time Objective (RTO)" means the maximum acceptable time for restoring system functionality following a disruption.

3. "Recovery Point Objective (RPO)" means the maximum acceptable period of data loss measured in time.

3. BACKUP REQUIREMENTS

1. Frequency and Retention

a) Full System Backups: Weekly

b) Incremental Backups: Every 4 hours

c) Transaction Logs: Real-time replication

d) Retention Period: 7 years for compliance data; 2 years for operational data

2. Storage Requirements

a) Primary backup storage must utilize encrypted, redundant storage arrays

b) Secondary backups must be maintained at geographically diverse locations

c) Tertiary backups must be stored in air-gapped environments

d) All backup media must implement AES-256 encryption

4. RECOVERY PROCEDURES

1. System Classification and RTO/RPO Requirements

System Category	RTO	RPO
Tier 1 Critical	15 minutes	0 minutes
Tier 2 Essential	2 hours	15 minutes
Tier 3 Supporting	8 hours	4 hours

2. Recovery Initiation Protocol

a) Incident Commander must authorize recovery procedures

b) Documentation of failure conditions required

c) Recovery team assembly within 10 minutes of authorization

d) Stakeholder notification per Communication Matrix

5. TESTING AND VALIDATION

1. Mandatory Testing Schedule

a) Full disaster recovery testing quarterly

b) Component recovery testing monthly

c) Backup integrity verification weekly

d) Restoration capability testing bi-weekly

2. Documentation Requirements

a) Test results must be logged in the Compliance Management System

b) Recovery time measurements must be recorded

c) Deviation reports must be generated for missed RTOs/RPOs

d) Remediation plans required for failed tests

6. ROLES AND RESPONSIBILITIES

1. Recovery Team Composition

- Recovery Director: Chief Technology Officer
- Technical Lead: VP of Engineering
- Security Lead: Chief Security Architect
- Operations Lead: Director of Infrastructure
- Compliance Monitor: Chief Compliance Officer

2. Team Member Requirements

a) Annual certification in recovery procedures

b) Quarterly tabletop exercise participation

c) On-call rotation participation

d) Cross-training in critical systems

7. COMPLIANCE AND REPORTING

1. All backup and recovery activities must comply with:

a) ISO 27001 requirements

b) NIST Cybersecurity Framework

c) Maritime cybersecurity regulations

d) Customer contractual obligations

2. Required Documentation

a) Monthly backup success rate reports

b) Quarterly recovery testing results

c) Annual procedure review documentation

d) Incident response logs

8. CONFIDENTIALITY

1. This document contains confidential and proprietary information of DeepShield Systems, Inc. Unauthorized disclosure, reproduction, or use is strictly prohibited.

9. AMENDMENTS AND REVIEWS

1. This procedure shall be reviewed annually by the Security Operations Committee.

2. Amendments require approval from:

a) Chief Technology Officer

b) Chief Security Architect

c) VP of Engineering

d) Chief Compliance Officer

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 1st day of January, 2024.

DEEPSHIELD SYSTEMS, INC.

By:

Sarah Blackwood

Chief Technology Officer

By:

Dr. Elena Rodriguez

Chief Security Architect

DOCUMENT CONTROL:

Last Review: December 15, 2023

Next Review: December 15, 2024

Document Owner: Security Operations Committee