DATA SECURITY PROTOCOL

DATA SECURITY PROTOCOL

AUTOMATED STORAGE SYSTEMS

Effective Date: January 15, 2024

Document Version: 2.1

Internal Reference: PDR-SEC-2024-001

1. PURPOSE AND SCOPE

1. This Data Security Protocol ("Protocol") establishes mandatory sec

2. This Protocol applies to all Company employees, contractors, and a

2. DEFINITIONS

1. "Automated Storage Systems" means all Company-operated roboti

2. "BlueCore(TM) Platform" refers to the Company's proprietary cold-

3. "Secure Operating Environment" means the controlled physical and

3. SYSTEM SECURITY REQUIREMENTS

1. Physical Security Controls

1.1. All Automated Storage Systems must be operated within designa

a) Multi-factor authentication access controls

b) 24/7 video surveillance

c) Environmental monitoring systems

d) Backup power systems

e) Temperature-hardened security infrastructure

1.2. Access to system maintenance ports and control interfaces shall

2. Digital Security Controls

2.1. All BlueCore(TM) Platform components must implement:

a) AES-256 encryption for data at rest

b) TLS 1.3 for data in transit

c) Secure boot verification

d) Real-time threat monitoring

e) Automated security logging

2.2. System access credentials must be managed through the Compa

4. OPERATIONAL PROCEDURES

1. System Access

1.1. Authorization for system access shall be granted on a least-privile

a) Written approval from department manager

b) Completion of security training

c) Signed confidentiality agreement

d) Background check clearance

1.2. Remote access to Automated Storage Systems must utilize Com

2. Data Management

2.1. All operational data generated by Automated Storage Systems sh

a) Classified according to Company data classification policy

b) Backed up daily to secure off-site storage

c) Retained according to legal requirements

d) Purged when no longer needed

2.2. System logs must be maintained for a minimum of 365 days and

a) Access attempts

b) Configuration changes

c) Security events

d) Performance metrics

5. INCIDENT RESPONSE

1. Security incidents involving Automated Storage Systems must be r

a) Information Security Officer

b) Chief Technology Officer

c) Chief Operating Officer

2. The Company's Incident Response Team shall:

a) Investigate all reported incidents

b) Document findings and corrective actions

c) Update security controls as needed

d) Provide incident reports to management

6. COMPLIANCE AND AUDIT

1. Quarterly security audits shall be conducted to verify compliance w

2. Annual penetration testing must be performed by qualified third-par

3. All audit findings requiring remediation shall be addressed within 30

7. PROTOCOL MAINTENANCE

1. This Protocol shall be reviewed and updated annually or upon signi

2. Updates require approval from:

a) Chief Technology Officer

b) Chief Information Security Officer

c) Chief Operating Officer

8. ENFORCEMENT

1. Violations of this Protocol may result in disciplinary action up to and

2. The Company reserves the right to restrict or revoke system access

AUTHORIZATION

APPROVED AND ADOPTED by the undersigned authorized represen

Dynamics Robotics, Inc.

Date: January 15, 2024

Marcus Chen

Chief Technology Officer

Sarah Nordstrom

Chief Operating Officer

Dr. Elena Frost

Chief Executive Officer