DATA PRIVACY AND SECURITY POLICY

Polar Dynamics Robotics, Inc.

Effective Date: January 1, 2024

Policy Version: 3.0

1. PURPOSE AND SCOPE

1 This Data Privacy and Security Policy (the "Policy") establishes the standards and procedures for protecting confidential information, trade secrets, and personal data processed by Polar Dynamics Robotics, Inc. (the "Company") in connection with its development, manufacture, and deployment of autonomous mobile robots and related technologies.

2 This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel ("Covered Persons") who have access to Company systems, networks, or data.

2. DEFINITIONS

1 "Confidential Information" means proprietary technical data, trade secrets, know-how, research, product plans, customer data, or other sensitive information related to the Company's IceNav(TM) platform, thermal management systems, and robotics technologies.

2 "Personal Data" means any information relating to an identified or identifiable natural person, including but not limited to employee records, customer contact information, and user telemetry data collected from deployed AMR units.

3 "Security Incident" means any actual or suspected unauthorized access, disclosure, use, alteration, or destruction of Confidential Information or Personal Data.

3. DATA CLASSIFICATION AND HANDLING

1 The Company classifies data into the following categories:

- Level 1: Public Information
- Level 2: Internal Use Only
- Level 3: Confidential
- Level 4: Highly Confidential/Trade Secrets

2 All technical specifications, source code, and algorithmic models related to the Company's

cold-resistant actuator technology and IceNav(TM) platform are classified as Level 4 data requiring maximum security controls.

3 Customer deployment data, performance metrics, and operational telemetry are classified as Level 3 data requiring enhanced security measures.

4. SECURITY CONTROLS AND SAFEGUARDS

1 Technical Controls

- Multi-factor authentication for all system access
- End-to-end encryption for data in transit and at rest
- Network segmentation and monitoring
- Regular security patches and updates
- Automated threat detection and response

2 Physical Controls

- Biometric access controls for R&D facilities
- Secure disposal of physical media
- Clean desk policy
- Visitor management procedures
- Environmental controls for server rooms

3 Administrative Controls

- Annual security awareness training
- Background checks for employees
- Regular security assessments
- Incident response procedures
- Change management protocols

5. DATA RETENTION AND DISPOSAL

1 The Company shall retain data only as long as necessary for business purposes or as required by law, following these minimum retention periods:

- Technical development records: 7 years
- Customer contracts and deployment data: 5 years

- Employee records: 3 years post-employment
- Security logs and access records: 2 years

2 Data disposal must follow secure destruction procedures appropriate to the data classification level and medium type.

6. INCIDENT RESPONSE AND REPORTING

1 All Covered Persons must immediately report suspected Security Incidents to the Information Security Team at security@polardynamics.com or via the confidential reporting hotline.

2 The Incident Response Team shall:

- Investigate and contain the incident
- Document the incident and response actions
- Notify affected parties as required by law
- Implement corrective measures
- Update security controls as needed

7. COMPLIANCE AND ENFORCEMENT

1 Violation of this Policy may result in disciplinary action up to and including termination of employment or service relationship.

2 The Company reserves the right to monitor and audit compliance with this Policy.

3 This Policy shall be reviewed annually and updated as necessary to reflect changes in technology, business operations, or legal requirements.

8. EXCEPTIONS AND MODIFICATIONS

1 Exceptions to this Policy must be approved in writing by both the Chief Technology Officer and Chief Information Security Officer.

2 The Company reserves the right to modify this Policy at any time with notice to Covered Persons.

ACKNOWLEDGMENT

I acknowledge that I have read and understand this Data Privacy and Security Policy and agree to

comply with its terms.

```

**Name: _**

**Title: _**

**Date: _**

**Signature: _**

```

End of Policy