NETWORK SECURITY ARCHITECTURE DOCUMENT

Polar Dynamics Robotics, Inc.

Document Version: 2.4

Last Updated: January 11, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION

1 This Network Security Architecture Document ("Architecture Document") sets forth the comprehensive network security infrastructure and protocols implemented by Polar Dynamics Robotics, Inc. ("Company") to protect its proprietary autonomous mobile robot ("AMR") systems, IceNav(TM) platform, and related technological assets.

2 This document is classified as CONFIDENTIAL and contains trade secrets and proprietary information of the Company.

2. NETWORK ARCHITECTURE OVERVIEW

1 **Core Infrastructure**

- Segmented network architecture with distinct zones for:
- AMR Development Environment
- Production Systems
- Corporate Operations
- Customer Data Processing
- IceNav(TM) Platform Infrastructure

2 **Security Zones**

- DMZ configuration for external-facing services
- Isolated development environment for robotics programming
- Segregated networks for thermal management systems
- Dedicated VLAN for cold-environment testing facilities
- Air-gapped networks for proprietary actuator technology development

3. ACCESS CONTROL SYSTEMS

1 **Authentication Infrastructure**

- Multi-factor authentication (MFA) required for all network access
- Biometric verification for critical systems access
- Role-based access control (RBAC) implementation
- Privileged Access Management (PAM) system
- Zero-trust architecture for remote access

2 **Identity Management**

- Centralized identity provider (IdP) integration
- Regular access rights review and certification
- Automated de-provisioning protocols
- Secure credential vault implementation

4. DATA PROTECTION MECHANISMS

1 **Encryption Standards**

- AES-256 encryption for data at rest
- TLS 1.3 for all data in transit
- End-to-end encryption for AMR command and control
- Hardware security modules (HSM) for key management
- Quantum-resistant encryption protocols for critical systems

2 **Data Classification**

- Proprietary IceNav(TM) algorithms: Restricted
- Customer telemetry data: Confidential
- Thermal management specifications: Restricted
- Operational logs: Internal Use Only
- Development documentation: Confidential

5. SECURITY MONITORING AND RESPONSE

1 **Security Operations Center (SOC)**

- 24/7 monitoring of network infrastructure
- Advanced threat detection systems

- Security information and event management (SIEM) implementation
- Automated incident response protocols
- Real-time AMR security telemetry analysis

2 **Incident Response**

- Documented incident response procedures
- Designated incident response team
- Regular tabletop exercises
- Forensics capability maintenance
- Customer notification protocols

6. COMPLIANCE AND AUDIT

1 **Regulatory Compliance**

- ISO 27001 certification maintenance
- SOC 2 Type II compliance
- GDPR compliance for EU operations
- CCPA compliance for California operations
- Industry-specific security standards adherence

2 **Audit Procedures**

- Quarterly internal security audits
- Annual third-party penetration testing
- Continuous compliance monitoring
- Regular vulnerability assessments
- Security control effectiveness reviews

7. BUSINESS CONTINUITY

1 **Disaster Recovery**

- Geographically distributed backup systems
- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 15 minutes
- Regular disaster recovery testing

- Automated failover capabilities

2 **Redundancy**

- N+1 redundancy for critical systems
- Multi-region cloud infrastructure
- Redundant network connectivity
- Backup power systems
- Alternative command and control centers

8. VENDOR MANAGEMENT

1 **Third-Party Security**

- Vendor security assessment program
- Regular security reviews of critical vendors
- Contractual security requirements
- Vendor access monitoring
- Security SLA enforcement

9. DOCUMENT CONTROL

1 This document shall be reviewed and updated annually or upon significant changes to network architecture.

2 Distribution of this document is restricted to authorized personnel only.

3 Document owner: Chief Information Security Officer

10. APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Network Security Architecture Document has been approved and adopted by the authorized representatives of Polar Dynamics Robotics, Inc.

APPROVED BY:

Marcus Chen

Chief Technology Officer

Date: January 11, 2024

Katherine Wells

Chief Financial Officer

Date: January 11, 2024

Dr. Elena Frost

Chief Executive Officer

Date: January 11, 2024