IceNav User Authentication Protocol

Document ID: PDR-SEC-2023-441

Version: 3.2

Effective Date: January 15, 2024

Classification: CONFIDENTIAL

1. Purpose and Scope

1. This User Authentication Protocol ("Protocol") establishes the security requirements and procedures for user authentication within the IceNav Autonomous Navigation System ("IceNav System") developed and maintained by Polar Dynamics Robotics, Inc. ("Company").

2. This Protocol applies to all authorized users accessing the IceNav System, including but not limited to employees, contractors, system administrators, and authorized client personnel.

2. Definitions

1. "Authentication Credentials" means the unique identifiers and verification elements required for system access, including user IDs, passwords, biometric data, and security tokens.

2. "Multi-Factor Authentication" or "MFA" means the security process requiring two or more independent authentication methods.

3. "Security Token" means a physical or digital device that generates time-based one-time passwords (TOTP) for additional authentication verification.

4. "System Administrator" means personnel designated by the Company with elevated access privileges to manage the IceNav System.

3. Authentication Requirements

1. Basic Authentication

a) All users must maintain unique user IDs assigned by the System Administrator

b) Passwords must meet the following criteria:

- Minimum length of 12 characters
- Include uppercase and lowercase letters

- Include at least one number and special character
- Cannot match previous 10 passwords
- Must be changed every 90 days

2. Multi-Factor Authentication

a) MFA is mandatory for all user access

b) Primary authentication requires password entry

c) Secondary authentication requires either:

- Company-issued security token
- Biometric verification via approved device
- SMS verification to registered device

3. Session Management

a) Automatic session timeout after 15 minutes of inactivity

b) Maximum session duration of 8 hours

c) Concurrent sessions limited to two per user

4. Access Levels and Privileges

1. Standard User Access

- Basic robot operation functions
- Navigation path viewing
- Performance metrics access
- Personal profile management

2. Advanced User Access

- Path programming capabilities
- Basic configuration changes
- Performance optimization tools
- Team management functions

3. Administrator Access

- Full system configuration
- User management

- Security protocol modification
- Audit log access

5. Security Protocols

1. Failed Authentication Handling

a) Account lockout after 5 failed attempts

b) 30-minute lockout duration

c) System Administrator notification of lockouts

d) Mandatory security review for repeated failures

2. Authentication Logging

a) All authentication attempts logged

b) Log entries include:

- Timestamp
- User ID
- IP address
- Authentication method
- Success/failure status

3. Emergency Access Procedures

a) Documented emergency override protocols

b) Dual administrator authorization required

c) Automatic notification to Security Team

d) Maximum 4-hour duration for emergency access

6. Compliance and Audit

1. Regular compliance audits conducted quarterly

2. Authentication logs retained for 180 days

3. Annual penetration testing of authentication systems

4. Bi-annual review and update of this Protocol

7. Enforcement and Violations

1. Violation of this Protocol may result in:

a) Immediate access suspension

b) Disciplinary action

c) Legal action where applicable

d) Termination of employment or contract

8. Protocol Modifications

1. This Protocol may be modified only by written authorization from:

a) Chief Technology Officer

b) Chief Information Security Officer

c) Chief Robotics Officer

9. Legal Notice

This Protocol is confidential and proprietary to Polar Dynamics Robotics, Inc. Unauthorized disclosure, copying, or distribution is strictly prohibited and may result in civil and criminal penalties.

Approval and Implementation

APPROVED AND ADOPTED this 15th day of January, 2024.

POLAR DYNAMICS ROBOTICS, INC.

By:

Marcus Chen

Chief Technology Officer

By:

Dr. James Barrett

Chief Robotics Officer