WIRELESS COMMUNICATION SECURITY PROTOCOL

WIRELESS COMMUNICATION SECURITY PI

NaviFloor Robotics, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Security Classification: Confidential

1. PURPOSE AND SCOPE

-

1. This Wireless Communication Security Protocol ("Protocol") establishes t

-

2. This Protocol applies to all wireless communication systems utilized in the

a) Robot-to-Robot (R2R) Communications

b) Robot-to-Infrastructure (R2I) Communications

c) Fleet Management System Communications

d) Remote Monitoring and Control Systems

e) Emergency Override Systems

2. DEFINITIONS

-

1. "Secure Channel" means an encrypted communication pathway utilizing A

-

2. "Critical Commands" means any wireless instruction that affects robot mo

-

3. "Authentication Token" means a unique identifier assigned to each AMR u

-

4. "Network Zone" means a designated operational area within which specifi

3. TECHNICAL REQUIREMENTS

-

1. Encryption Standards

a) All wireless communications must utilize minimum AES-256 encryption

b) Key rotation shall occur every 24 hours or upon detection of potential security breach

c) Encryption keys shall be stored in tamper-resistant hardware modules

-

2. Authentication Protocols

a) Multi-factor authentication required for all administrative access

b) Certificate-based mutual authentication for all R2R communications

c) Hardware-based security tokens for critical system access

-

3. Network Segmentation

a) Separate VLAN implementation for each customer deployment

b) Air-gapped networks for critical control systems

c) Dedicated emergency override channels

4. OPERATIONAL PROCEDURES

-

1. Communication Initialization

a) Automated handshake verification required before establishing connection

b) Maximum three retry attempts before security lockout

c) Mandatory logging of all connection attempts

-

2. Monitoring and Alerts

a) Real-time monitoring of all wireless communication channels

b) Automated alerts for unauthorized access attempts

c) Weekly security audit reports

-

3. Emergency Protocols

a) Redundant communication pathways for critical commands

b) Fail-safe modes for communication loss scenarios

c) Manual override capabilities via secure physical interface

5. COMPLIANCE AND TESTING

-

1. Regular Testing Requirements

a) Monthly penetration testing of wireless systems

b) Quarterly security protocol validation

c) Annual third-party security audit

-

2. Documentation Requirements

a) Maintenance of detailed security logs for 365 days

b) Documentation of all security incidents and resolutions

c) Regular updates to security procedures based on test results

6. PROPRIETARY RIGHTS AND CONFIDENTIALIT

-

1. All wireless communication protocols, encryption methods, and security m

-

2. Disclosure of this Protocol or its contents is strictly prohibited except as re

7. AMENDMENTS AND UPDATES

-

1. This Protocol may be amended or updated by the Company's Technology

-

2. All amendments shall be documented and communicated to relevant perso

8. ENFORCEMENT

-

1. Violation of this Protocol may result in immediate system access terminati

-

2. The Company reserves the right to pursue legal action for any breach of th

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Protocol has been reviewed and approved by undersigned authorized representatives of NaviFloor Robotics, Inc.

APPROVED BY:

Marcus Depth

Chief Technology Officer

Date: January 15, 2024

Dr. Elena Kovacs

Chief Research Officer

Date: January 15, 2024

Richard Torres

Chief Operating Officer

Date: January 15, 2024