NAVIFLOOR CLOUD INTEGRATION ARCHITECTURE

NAVIFLOOR CLOUD INTEGRATION ARCHI

Document Version: 3.2

Last Updated: January 11, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

-

1. This Cloud Integration Architecture document ("Architecture Document")

-

2. This document shall be governed by and construed in accordance with the

2. DEFINITIONS

-

1. "Cloud Services" means the Company's cloud-based infrastructure and ser

-

2. "Integration Points" refers to the authorized connection points between the

-

3. "Platform" means the Company's proprietary AMR fleet management soft

-

4. "Security Protocol" means the comprehensive set of security measures anc

3. CLOUD ARCHITECTURE OVERVIEW

-

1. Primary Infrastructure

-

Primary cloud provider: Amazon Web Services (AWS)

-

Secondary redundancy: Microsoft Azure

-

Geographic distribution: US East (Primary), US West (Secondary), EU Cent

-

2. Service Components

-

Containerized microservices architecture using Kubernetes

-

Real-time data processing through Apache Kafka

-

Terrain mapping data storage in MongoDB Atlas

-

LiDAR processing pipeline hosted on dedicated instances

4. INTEGRATION REQUIREMENTS

-

1. API Specifications

-

RESTful APIs using OpenAPI 3.0 specification

-

GraphQL endpoints for complex data queries

-

WebSocket connections for real-time robot telemetry

-

OAuth 2.0 authentication with JWT tokens

-

2. Customer Integration Points

-

Secure VPN tunnels for on-premises connections

-

MQTT brokers for robot-to-cloud communication

-

Custom SSL certificates for customer domains

-

API rate limiting and throttling mechanisms

5. SECURITY ARCHITECTURE

-

1. Data Protection

-

AES-256 encryption for data at rest

-

TLS 1.3 for data in transit

-

Customer data isolation through dedicated database schemas

-

Regular penetration testing and security audits

-

2. Access Control

- Role-based access control (RBAC)

- Multi-factor authentication for administrative access

- IP whitelisting for production environments

- Audit logging of all system access

6. COMPLIANCE AND CERTIFICATIONS

- 1. The Cloud Services shall maintain compliance with:

- ISO 27001:2013

-

SOC 2 Type II

-

GDPR (where applicable)

-

Industry-specific standards as required by customers

-

2. Annual third-party audits shall be conducted to verify compliance.

7. DISASTER RECOVERY AND BUSINESS CONTINU

-

1. Recovery Time Objectives (RTO)

-

Critical systems: 4 hours

-

Non-critical systems: 12 hours

-

2. Recovery Point Objectives (RPO)

-

Critical data: 15 minutes

-

Non-critical data: 4 hours

-

3. Backup Procedures

-

Daily incremental backups

-

Weekly full backups

-

Cross-region replication

-

Monthly disaster recovery testing

8. PROPRIETARY RIGHTS AND CONFIDENTIALIT

-

1. All aspects of the Cloud Integration Architecture, including but not limite

-

2. This document may not be disclosed to third parties without explicit writte

9. MODIFICATIONS AND UPDATES

-

1. This Architecture Document may be modified or updated by the Company

-

2. Material changes shall require approval from the Company's Architecture

10. EXECUTION AND APPROVAL

IN WITNESS WHEREOF, this Cloud Integration Architecture document ha reviewed and approved by the undersigned authorized representatives of the Company.

NAVIFLOOR ROBOTICS, INC.

By:

Name: Marcus Depth

Title: Chief Technology Officer

Date: January 11, 2024

By:

Name: Dr. Elena Kovacs

Title: Chief Research Officer

Date: January 11, 2024