Security Documentation for Fleet Vision

Cristian Paul P. Loria
c.loria.537000@umindanao edu,ph

Myko Xiren D. Dungca
m.dungca.536774@uminda nao.edu.ph

Dave Christian M. Morales
d.morales.534812@uminda nao.edu.ph

1. Introduction

1.1 Overview

Fleet Vision is a transportation management system designed to optimize routes, manage deliveries, and improve communication between drivers and clients. It helps businesses streamline their operations by providing real-time tracking, efficient scheduling, and automated notifications.

1.2 Purpose

This security documentation is crucial to ensure that Fleet Vision operates in a secure environment. It aims to protect the system from unauthorized access, safeguard sensitive data, and maintain system availability.

1.3 Scope

This document covers security aspects of Fleet Vision, including data protection, system architecture, user authentication, and incident response procedures. It does not address general application features unrelated to security.

2. Security Goals and Objectives

The key security goals of Fleet Vision are to ensure the confidentiality, integrity, and availability of the system. The system should only allow authorized users to access and modify data, ensure data is not tampered with, and be available for use at all times. Authentication must be secure, and users must not be able to deny actions they have taken.

3. Security Architecture

3.1 System Overview

Fleet Vision is built with a layered security approach, using both frontend and backend components. The backend is developed using ASP.NET Core and integrates with SQL Server for database management. The system utilizes role-based access control to grant different levels of access to users, such as admins, drivers, and customers.

3.2 Data Flow

Data in Fleet Vision moves through secure channels. User data is encrypted during transmission using SSL/TLS, ensuring no data is intercepted or altered during transit. Sensitive data like passwords is hashed before being stored in the database.

3.3 Security Technologies

Fleet Vision leverages modern security frameworks and tools. It uses SSL/TLS for encryption during data transmission, OAuth 2.0 or JWT Tokens for user authentication, and integrates with Google Maps API and Twilio API for service functionality.

4. Authentication and Authorization

4.1 Authentication Methods

To ensure secure access, Fleet Vision uses OAuth 2.0 or JWT Tokens for authentication. These methods help verify the identity of users before granting access to the system.

4.2 Access Control

Access control is implemented using role-based access control (RBAC). Different user roles, such as admins, drivers, and customers, are granted specific permissions. Admins have full access, while drivers and customers have limited permissions based on their roles.

5. Data Protection

5.1 Data Encryption

Data protection is enforced by using SSL/TLS for encrypting information as it travels over the internet. Sensitive data like passwords and payment details are hashed in the database using algorithms like bcrypt or SHA-256.

5.2 Privacy Compliance

Fleet Vision ensures compliance with privacy regulations like GDPR. This includes data protection measures and giving users control over their personal data.

6. Secure Development Practices

6.1 Coding Standards

[Fleet Vision follows secure coding practices, such as adhering to the OWASP Top 10 standards. This helps prevent common security vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

6.2 Security Testing

Security testing is performed through regular code reviews, automated security tools, and manual penetration testing. This ensures vulnerabilities are identified and fixed before they can be exploited.

7. Vulnerability Management

Vulnerability scanning is performed regularly to detect potential weaknesses in the system. Penetration testing is also conducted to ensure the system can withstand common attacks.

8. Incident Response Plan

An incident response plan is in place to quickly detect and respond to security breaches. The plan includes steps for identifying the cause, containing the breach, and recovering the system.

9. Deployment and Infrastructure Security

Security measures are in place for the deployment of Fleet Vision, including secure CI/CD pipelines, firewalls, and DDoS protection. The application is hosted on Hostinger, which provides cloud-based infrastructure with enhanced security features.

10. Monitoring and Logging

System activity is monitored using centralized logging tools like Serilog or the ELK Stack. Azure Monitor is used to detect anomalies and performance issues, ensuring the system is operating securely and efficiently.

11. Security Compliance and Certifications

Fleet Vision complies with several industry standards, including ISO 27001 and SOC 2, to ensure it meets security best practices and regulatory requirements.

12. User Security Awareness

To protect users, Fleet Vision educates them about security best practices, such as using strong passwords and avoiding phishing attempts. Security prompts and reminders are provided to help users follow these practices.

13. Review and Update Policy

The security documentation for Fleet Vision is reviewed annually or whenever significant changes to the system occur. This ensures the security measures remain up-to-date and effective against evolving threats.