
SOFTWARE REQUIREMENTS SPECIFICATION IEEE 830

for

Zenith PWA
Version 1.0

Prepared by : García Gonzalez Christian Andrés
López Bautista Cristian Alexis
Mercado Juárez Ángel Hayr
Salas Díaz Guillermo
Santillán Galavíz Ken Antonio

Submitted to : Dr. Ray Brunet Parra Galaviz

February 6, 2024

Contents

1	Introduction	4
1.1	Purpose	4
1.2	Intended Audience and Reading Suggestions	4
1.3	Project Scope	4
2	Overall Description	6
2.1	Product Perspective	6
2.2	User Classes and Characteristics	6
2.3	Product Functions	6
2.4	Operating Environment	7
2.5	Design	7
3	System Features	9
3.1	Description and Priority	9
3.2	Functional Requirements	9
3.2.1	User Authentication and Authorization	9
3.2.2	Employee Data Management	10
3.2.3	Incident Reporting	10
3.2.4	Data Visualization	10
3.2.5	QR Code Scanning	10
4	Other Nonfunctional Requirements	11
4.1	Performance Requirements	11
4.1.1	Response Time	11
4.1.2	Scalability	11
4.2	Security Requirements	11
4.2.1	Data Encryption	11
4.2.2	User Authentication	11
4.2.3	Authorization Controls	11
4.2.4	Incident Report Security	11
4.3	Software Quality Attributes	12
4.3.1	Usability	12
4.3.2	Reliability	12
4.3.3	Maintainability	12
4.4	Business Rules	12
4.4.1	Incident Reporting	12
4.4.2	Data Accuracy	12

5	Other Requirements	13
5.1	Cross-Browser Compatibility	13
5.2	Mobile Device Compatibility	13
5.3	Training and Documentation	13

1 Introduction

1.1 Purpose

The purpose of the "Zenith" project is to develop a Progressive Web Application (PWA) that extends the existing web platform's capabilities, specifically tailored for the use of businesses. The application aims to provide a comprehensive solution for managing and analyzing employee data, including personal and health information. The primary goal is to facilitate efficient incident reporting related to employees, covering both illnesses and workplace accidents. By leveraging the platform, organizations can maintain a centralized record of incidents and utilize graphical representations and tables for streamlined review and analysis.

1.2 Intended Audience and Reading Suggestions

The primary audience for the "Zenith" PWA includes businesses and organizations seeking an integrated solution for employee data management and incident reporting. This encompasses various stakeholders, such as human resources personnel, safety officers, and healthcare professionals within the organization. Additionally, those responsible for overseeing employee well-being and safety, such as nurses and health aides, will find the mobile capabilities of the application particularly beneficial.

Reading suggestions for this document are as follows:

- Business executives and decision-makers: Focus on the overarching goals and benefits of the "Zenith" PWA in enhancing employee data management and incident reporting within the organization.
- Technical teams and developers: Explore the detailed specifications and requirements outlined in subsequent sections to understand the technical aspects of implementing the PWA.
- End users: Gain insights into the user experience and functionalities of the "Zenith" PWA, particularly if involved in incident reporting or data management.

1.3 Project Scope

The scope of the "Zenith" PWA project encompasses the development and deployment of a user-friendly and efficient platform for managing employee data and incident reporting.

Key features include:

- **Employee Data Management:** Capture and store comprehensive employee information, including personal details, health data (e.g., blood type, allergies), and relevant contact information.
- **Incident Reporting:** Enable users to quickly and seamlessly report incidents through the mobile application, including details of illnesses and workplace accidents.
- **Data Visualization:** Provide graphical representations and tabular views of incident data for easy review and analysis by authorized personnel.
- **Mobile Accessibility:** Extend the platform's accessibility to mobile devices, allowing healthcare professionals and safety officers to scan unique employee QR codes for instant access to relevant information and incident reporting capabilities.

The "Zenith" PWA aims to enhance organizational efficiency, data accuracy, and emergency response by offering a comprehensive and accessible solution for managing employee information and incident reporting.

2 Overall Description

2.1 Product Perspective

The "Zenith" PWA is designed as an extension of the existing "Zenith" web platform, creating a seamless and integrated experience for users. The PWA interacts with the same backend infrastructure and database, ensuring consistency and real-time data synchronization between the web and mobile interfaces. The PWA is a self-contained system, but it relies on the web platform's data storage and processing capabilities.

2.2 User Classes and Characteristics

The "Zenith" PWA caters to different user classes with varying roles and responsibilities within an organization:

- **Administrators:** Responsible for managing overall system settings, user access, and overseeing the integration with the existing web platform.
- **Healthcare Professionals:** Including nurses and health aides, these users focus on accessing and updating employee health information, as well as utilizing the incident reporting feature for quick response.
- **Safety Officers:** Tasked with monitoring and managing workplace safety, safety officers utilize the platform to review incident reports, analyze trends, and take preventive measures.
- **Employees:** Regular employees use the PWA to access their personal information, including health details, and report incidents quickly through the mobile interface.

2.3 Product Functions

The "Zenith" PWA incorporates the following key functions:

- **User Authentication and Authorization:** Ensures secure access to the platform, with varying levels of permissions based on user roles.
- **Employee Data Management:** Allows administrators to add, modify, and delete employee information, including personal details and health-related data.

- **Incident Reporting:** Enables users to swiftly report incidents, providing details such as type of incident, location, and a brief description. Notifications are sent automatically to designated emergency contacts.
- **Data Visualization:** Presents graphical representations and tabular views of incident data, supporting trend analysis and decision-making.
- **QR Code Scanning:** Facilitates mobile accessibility by allowing healthcare professionals and safety officers to scan unique employee QR codes, providing instant access to relevant information and incident reporting features.

2.4 Operating Environment

The "Zenith" PWA operates in a web-based environment and is compatible with modern web browsers, ensuring accessibility across various devices and platforms. The application is designed to function efficiently in both online and offline modes, providing a seamless user experience even in low-connectivity scenarios.

2.5 Design

The design of the "Zenith" PWA focuses on an intuitive and user-friendly interface, ensuring a positive user experience.



Figure 2.1: Zenith splash screen, QR scanning and charts.

The mobile interface is optimized for responsiveness, allowing users to navigate and utilize features effortlessly on devices of varying screen sizes. Given the dynamic nature of security operations, personnel often need to access critical information on the go. The adaptability of our PWA to various mobile devices ensures that security consultations can be conducted seamlessly on smartphones and tablets, providing flexibility and efficiency in daily tasks.

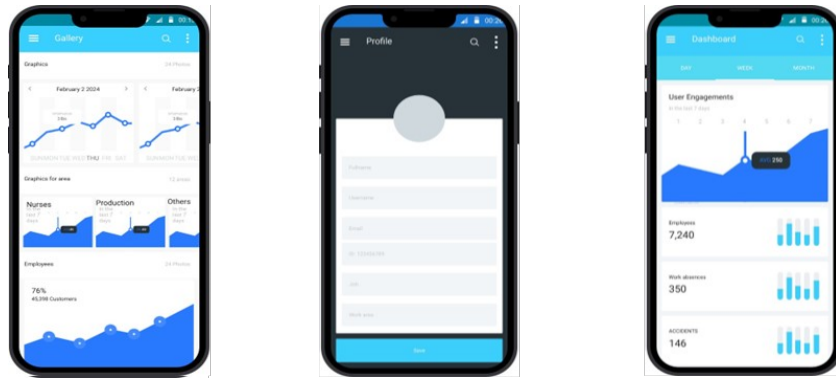


Figure 2.2: Zenith user data and profile page.

The overall design adheres to industry best practices for security, scalability, and maintainability to support the long-term success of the platform.

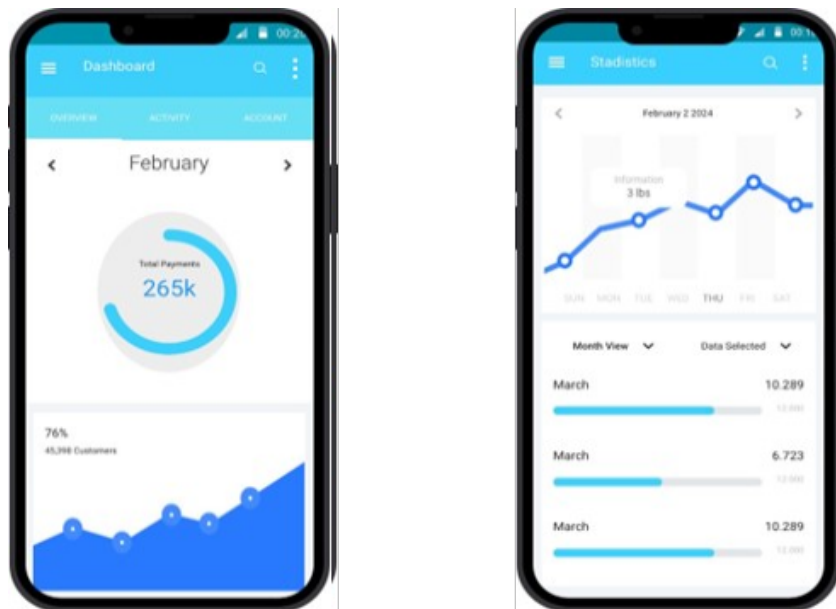


Figure 2.3: Zenith dashboards.

3 System Features

3.1 Description and Priority

The "Zenith" PWA encompasses several key features crucial for efficient employee data management and incident reporting. Each feature is prioritized based on its significance to the overall functionality of the platform.

- User Authentication and Authorization (Priority: High): Securely authenticate users and assign appropriate access levels based on their roles. Ensures data privacy and system integrity.
- Employee Data Management (Priority: High): Allows administrators to add, modify, and delete employee information, including personal details and health-related data. Ensures accurate and up-to-date records.
- Incident Reporting (Priority: High): Enables users to quickly report incidents, providing essential details such as incident type, location, and a brief description. Automatic notifications are sent to designated emergency contacts for swift response.
- Data Visualization (Priority: Medium): Presents incident data through graphical representations and tabular views, facilitating trend analysis and informed decision-making by safety officers and administrators.
- Code Scanning (Priority: Medium): Facilitates mobile accessibility by allowing healthcare professionals and safety officers to scan unique employee QR codes. Provides instant access to employee information and incident reporting features.

3.2 Functional Requirements

3.2.1 User Authentication and Authorization

- Requirement 1: Users must register with a valid email and password.
- Requirement 2: The system must verify user credentials securely before allowing access.
- Requirement 3: Different user roles (Administrator, Healthcare Professional, Safety Officer, Employee) must have distinct permissions.

3.2.2 Employee Data Management

- Requirement 4: Administrators can add new employees, capturing personal details and health-related information.
- Requirement 5: Employee information must be editable to accommodate changes in personal or health data.
- Requirement 6: Administrators can delete employee records, ensuring data accuracy and compliance.

3.2.3 Incident Reporting

- Requirement 7: Users can initiate incident reports, providing details such as incident type, location, and description.
- Requirement 8: The system must timestamp and store incident reports securely in the database.
- Requirement 9: Automated notifications must be sent to designated emergency contacts upon the submission of an incident report.

3.2.4 Data Visualization

- Requirement 10: The system must generate graphical representations (charts, graphs) of incident data for easy visualization.
- Requirement 11: Tabular views of incident data must be available for detailed analysis.
- Requirement 12: Authorized users can apply filters for customized views based on parameters such as date, incident type, or employee.

3.2.5 QR Code Scanning

- Requirement 13: The PWA must support QR code scanning functionality for quick access to employee information.
- Requirement 14: Scanned QR codes must provide healthcare professionals and safety officers with access to incident reporting features.

These functional requirements ensure the successful implementation of core features within the "Zenith" PWA, addressing the needs of various user classes and contributing to a comprehensive employee data management and incident reporting system.

4 Other Nonfunctional Requirements

4.1 Performance Requirements

4.1.1 Response Time

- Requirement 1: The "Zenith" PWA should provide a responsive user interface, with an average response time of no more than 2 seconds for standard operations.

4.1.2 Scalability

- Requirement 2: The system must handle a scalable number of users, supporting simultaneous access by at least 500 users without significant degradation in performance.

4.2 Security Requirements

4.2.1 Data Encryption

- Requirement 3: All communication between the PWA and the backend system must be encrypted using secure protocols (e.g., HTTPS) to ensure data confidentiality.

4.2.2 User Authentication

- Requirement 4: User authentication must comply with industry best practices, including secure password storage and protection against common authentication vulnerabilities.

4.2.3 Authorization Controls

- Requirement 5: The system must enforce role-based access controls, ensuring that each user can only access features and data relevant to their assigned role.

4.2.4 Incident Report Security

- Requirement 6: Incident reports must be stored securely, and access to this sensitive information must be restricted to authorized personnel.

4.3 Software Quality Attributes

4.3.1 Usability

- Requirement 7: The PWA must be designed with a user-friendly interface, ensuring ease of navigation and a positive user experience for individuals with varying levels of technical proficiency.

4.3.2 Reliability

- Requirement 8: The system must have a high level of reliability, with an expected uptime of at least 99% to minimize disruptions to user access.

4.3.3 Maintainability

- Requirement 9: The codebase must be well-documented, and the system architecture should allow for easy maintenance and updates without significant downtime.

4.4 Business Rules

4.4.1 Incident Reporting

- Requirement 10: Employees are required to report any work-related incidents within 24 hours of occurrence.
- Requirement 11: Incident reports must include accurate and detailed information to be considered valid.

4.4.2 Data Accuracy

- Requirement 12: Employee data must be reviewed and updated by administrators annually to ensure accuracy.
- Requirement 13: Inaccurate or outdated data must be corrected promptly upon identification.

5 Other Requirements

5.1 Cross-Browser Compatibility

- Requirement 1: The PWA should be compatible with popular web browsers, including but not limited to Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge, to ensure a consistent user experience.

5.2 Mobile Device Compatibility

- Requirement 2: The PWA must be optimized for mobile devices, supporting various screen sizes and resolutions to facilitate ease of use on smartphones and tablets.

5.3 Training and Documentation

- Requirement 3: Comprehensive training materials and documentation must be provided to assist users in understanding the functionalities of the PWA, promoting efficient system usage.