# Documentation of requirements software

*[staff-access-monitoring-system]*

***Date:** [01/09/2024]*

# Content

## Project information

| | |
|---|---|
| **Organization** | Computer laboratory - FCEFYN |
| **Project** | Staff access monitoring system |
| **Start date** | 01/09/2024 |
| **Client** | School of Computer Engineering UNC |
| **Sponsor** | Laboratory Director |
| **Project Leader** | Gabriel Valenzuela |

## 1. Purpose and Product Scope

This project is a prototype of a Staff Access Monitoring System. The project seeks to design and develop a prototype to accurately record entries and exits in the Computer Lab. The system will capture biometric data, link it to each person and store the information on a remote server. It will also have a simple web page for administrators.

This documentation covers user requirements such as the interface and functional requirements such as connectivity, terminals and project deployment.

The objective of the project is to cover the laboratory's need to have more rigorous control for the use of the laboratory facilities, monitoring access to the physical space. In addition, the project seeks to cover the objectives of a "PPS" of the Computer Engineering degree.

## 2. System Features

- User profiles with the ability to assign different permissions, groups, etc.
- Logging of entry and exit date and time.
- Registration through biometric data (fingerprint).
- Remote firmware updates via Ethernet.
- Support for multiple terminals.
- Secure storage of sensitive data (biometrics, passwords, etc.).

## 3. User Classes and Characteristics

This section categorizes the users who will interact with the system. Below is a list of typical user types, along with their characteristics:

- Frequent Users: users who access regularly, requiring frequent entry and exit logging.
- Administrative Users: responsible for managing user profiles, assigning permissions, and monitoring system health. They require full access to all system functionalities, including remote firmware updates and secure data management.

# 4. Functional requirements

## 4.1. Connectivity

- Must be connected to the internet via Ethernet

## 4.2. Lightweight Terminals

- Data processing is done server-side; terminals are responsible only for data collection and transmission.
- Must include a biometric fingerprint sensor and a display for basic user information.

## 4.3. Web Administration Interface

- Easy management of terminals (user registration, biometric data collection, etc.).
- Intuitive visualization of collected data (summaries, statistics, etc.).
- Alert systems for anomaly detection.
- Simple integration of new terminals.

## 4.4. Deployment:

- Implementation must follow best programming and development practices.
- Provide documentation.
- Ability to deploy in containerized environments (Docker).
- Support for Continuous Integration and Continuous Deployment (CI/CD).
- Testing coverage between 40% and 60%.