**Role title**: Software Developer

**Brief role description**: You will work as part of a team of developers to implement a specification provided by a business analyst.

# Personal objectives

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectives** | **Evidence provided in self-appraisal document** | **Sprint 1** | **Sprint 2** |
| **Choose the relevant technologies** | See procedure: CDP02 | ✓ |  |
| **Produce code according to specification and coding standards** | See procedure: CDP02 | ✓ | ✓ |
| **Bug fixing** | See procedure: CDP02 | ✓ | ✓ |
| **Collaboration** | See procedure: CDP06 | ✓ | ✓ |
| **Attendance** | See procedure: CDP01 | ✓ | ✓ |
| **Security Testing** | See procedure: CDP09 | ✓ | ✓ |

# Personal skills:

* Experience in at least one relevant programming language
* A good understanding of software engineering practices and tools
* Good at problem solving
* Proactive, self-motivated, logical and objective
* Ability to work well under pressure, as part of a team or alone

# Relevant Procedures

* CDP01 – Attendance
* CDP02 - Software engineering
* CDP06 – Collaboration
* CDP09 – Security Testing

**Procedure CDP02 – Software engineering**

# Choosing the relevant technologies

The project focuses on developing a secured and encrypted android application which is designed to improve the experience of visitors in the university. The application integrates multiple technologies to ensure its security and functionality.

**1. Firebase for Authentication and Registration**

**Technology Used:** Firebase Authentication

**Purpose:** Secure user registration and login.

**Relevance**

* Firebase provides a scalable and secure backend solution for user authentication.
* It Supports Two-factor authentication with future integration of multi-factor authentication (MFA).
* Ensures data security by encrypting user credentials and session tokens.

**Implementation**

* Firebase SDK is integrated into the Android app to manage user sign-up and login.
* Real-time database used to store encrypted user profiles.

**2. AES Encryption for Data Security**

**Technology Used:** Advanced Encryption Standard (AES)

**Purpose:** Securely encrypt sensitive user data.

**Relevance**

* AES is a widely recognized encryption standard used by governments and enterprises.
* Ensures that stored and transmitted data (e.g., user credentials, schedules) remain confidential.

**Implementation**

* AES-256 encryption applied to stored user data and session tokens.
* Encryption keys managed securely using Android’s Keystore system.

**3. Mapbox API for Navigation**

**Technology Used:** Mapbox SDK (MapView & Navigation Libraries)

**Purpose:** Provide turn-by-turn navigation within the university.

**Relevance**

* Mapbox offers high-performance, customizable maps and navigation.
* Supports real-time location tracking and route optimization.

**Implementation**

* Integrated Mapbox Android SDK to display interactive maps.
* Navigation library used to calculate routes from the user’s current location to university buildings.

**4. ML Kit for QR Code Scanning**

**Technology Used:** Google ML Kit (Barcode Scanning)

**Purpose:** Scan QR codes to access lab resources and track visitor frequency.

**Relevance:**

ML Kit provides on-device machine learning for fast, offline QR code scanning.

Enables seamless interaction with lab equipment via QR-triggered video playback.

Implementation:

ML Kit’s barcode scanning API integrated to detect and decode QR codes.

Scanned data triggers relevant actions (e.g., playing instructional videos).

**5. Backend Visitor Tracking System**

**Technology Used:** Firebase Realtime Database

**Purpose:** Monitoring the QR code scan frequency to track lab/resource usage.

**Relevance**

Provides analytics on visitor trends for administrative decision-making.

Stores scan data securely with Firebase’s encryption in transit.

**Implementation**

Each QR scan logs an entry in Firebase with timestamp and user ID.

Admin dashboard retrieves and visualises the visitor’s data.

**Conclusion**

These technologies were selected because these are in line with the project’s core requirements. Mapbox AI was selected instead of its alternative Google maps because of its navigational features and smooth performance in indoor/outdoor routing. The selection of ML Kit for QR Scanning. Firebase realtime tracking was used because of its secured data management. These technologies provide efficient foundation for the application’s seamless user experience.

# Implementing functional requirements

You should implement all functional requirements as per agreed specification, i.e. **every item on the current sprint’s Backlog, as agreed with project manager.**

## Use of Version Control

You should commit your code regularly to a **Version Control system**.

Please note that many other services offer student tariff (often free!), for example:

* <https://education.github.com/>
* <https://bitbucket.org/plans>

Version Control systems are a great place to **collaborate**. Developers can share code, comments, create issues/bug entries, etc. Make sure that you use these features where applicable for a higher grade.

## Commenting your code

Collaboration amongst developers is also greatly helped by the use of comments that explain certain key sections of your code. You should always comment the code written as part of this assessment.

## **What to submit**

* Source code listings, highlighting sections that **you** have produced
* GitHub commit logs showing **your** commits
* GitHub commit graphs showing **your** commits

All these could be in a report on implementing functional requirements (max 5 pages)

# Bug fixing

You should work with the Business Analyst and rest of the team to fix as many bugs as possible.

## **What to submit**

* Source code extracts showing specific amendments/fixes to your code.
* Screenshots showing contributions to GitHub “Issues”, comments, fixes etc.

All these could be in a report on Bugs Fixing (max 2 pages)

**Procedure CDP09 – IT Security**

# Security testing

You should create a **test plan** based on your research in order to fully test the application against the most common security threats.

You should then **perform some security testing**, either manually, or using an automated security testing tool.

## **What to submit**

* A written report (e.g. Word document, max 4 pages)
* Screenshots of contributions to GitHub issues

**Procedure CDP06 – Collaboration**

# Good collaboration

**Good communication** and **good collaboration** are essential to a project’s success, and central to this module.

## Using computer software to enable/facilitate collaboration

Project managers and other members of the team should use [Basecamp](https://basecamp.com/) when suitable in order to achieve a higher grade. **Evidence of usage should be included** as part of your self-appraisal.

## **What to submit**

* Screenshots of Basecamp conversations in which **you** actively participate.
* Screenshots showing files (designs, reports) that **you** shared with your team on Basecamp
* Screenshots of personal contributions to GitHub issues.
* Evidence of course attendance (register, certificate), and Word document summarising what was learnt and how it can be used on the project (max 500 words).
* Please use **template provided** for the above (Canvas/templates/collaboration)

Screenshots of Source Code:







