# Hazard Analysis
# SFWRENG 4G06

Team #7, Team FAAM, SweatSmart

Daniel Akselrod
Jonathan Avraham
Sophie Fillion
Sam McDonald

Table 1: Revision History

| **Revision Version** | **Date** | **Developer(s)** | **Change** |
|---|---|---|---|
| 0 | Oct 20, 2023 | Sam, Sophie, Daniel, Jonathan | First draft |

# Contents

# 1 Introduction

SweatSmart is an AI powered fitness application that generates workout plans with the aim to help users start or maintain their fitness journey. This system, like every system design, must ensure that all safety requirements are met. This document outlines the system boundaries and components in the scope of the hazard analysis for this system. A Failure Mode and Effect Analysis (FMEA) has been created to outline possible failures and how to deal with them to ensure safety of the system.

# 2 Scope and Purpose of Hazard Analysis

The hazard analysis for SweatSmart serves a crucial role in ensuring the safety, reliability, and security of the application. In its scope, we comprehensively examine the system's boundaries and components, critical assumptions, user interactions, additional safety requirements, and an Effect Analysis that could potentially pose risks to users or impact the application's functionality. The primary purpose is to not only guarantee the safety of the users, but also enhance their overall experience when using the system. This can be achieved by identifying and mitigating potential hazards, aligning with relevant safety standards and regulations, reducing risks, and providing a user-friendly environment. By conducting this analysis, we instill confidence in our stakeholders, promote transparency, and demonstrate our commitment to ensuring the safety and security of our users.

# 3 System Boundaries and Components

## 3.1 System Boundaries

### 3.1.1 User Interface Boundary

This is the boundary between the user and the system. It's where the user interacts with the app on their iOS device.

### 3.1.2 Application Boundary

This encompasses the mobile app itself, including its local storage, local processing, and any embedded AI models that might run on the device.

### 3.1.3 Network Boundary

This is the boundary between the mobile app and the backend system hosted on Azure. It includes the internet and any APIs or services the app communicates with.

### 3.1.4 Backend Boundary

This is the boundary around the Azure-hosted backend. It includes the servers, databases, AI processing units, and other backend components.

## 3.2 System Components - Mobile App

### 3.2.1 User Interface

The screens, buttons, and other UI elements that users interact with.

### 3.2.2 Local Storage

Where user preferences, cached data, and runtime memory is stored

#### 3.2.3 API Client

Making network requests to the backend, handling responses, and managing errors.

### 3.3 System Components - Backend System (Azure)

#### 3.3.1 App Service

Backend hosted web-application on Azure

#### 3.3.2 Azure KeyVault

Stores secret environment variables for correct configuration

#### 3.3.3 SQL Server

Hosts an SQL Database and manages connections/security

#### 3.3.4 SQL Database

Stores application data retaining to certain user/fitness info

#### 3.3.5 Authentication & Authorization Service

Ensures that only registered and authorized users can access endpoints using JWT authorization.

#### 3.3.6 AI Service

AI Model for generating/updating workouts Notification Service: Manages and sends notifications to users

## 4 Critical Assumptions

### 4.1 Azure is secure and safe

We are using Azure as our backend system database. We are assuming that it is a safe platform that cannot be hacked into. Thus, failures relating to the failure of the application itself will not be considered.

## 5 Failure Modes and Effects Analysis

The Failure Modes and Effects Analysis (FMEA) was used to identify hazards within the system to mitigate them accordingly with safety and security requirements. The FMEA table can be found below.

| Component | Failure Modes | Effects of Failure | Causes of Failure | Recommended action | SR | Ref. |
|---|---|---|---|---|---|---|
| Profile | Account not created | User unable to access core app functionality | a. Database failure | a. Display error message and prompt user to try again | a. EHR1 | H1-1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | User unable to log in | User unable to access their existing account and application data | a. Login credentials not stored properly in database | a. Provide option for user to reset their credentials | a. INR3 | H1-2 |
| | User unable to update preferences | Workout generation will not be effectively personalized | a. Database update failure<br>b. Front-end functionality failure | a. Display detailed error message to user | a. EHR1 | H1-3 |
| | User workout history is not updated | User will not be able to see their progress | a. Database failure | a. Upon database failure, store data locally until database failure is resolved. Regularly attempt to upload data to minimize time data is stored locally | a. INR4 | H1-4 |
| | User account unintentionally deleted | Complete loss of account information | a. Database failure | a. Databases should be regularly and automatically backed up with the opportunity to rollback changes given a database failure. | a. INR3 | H1-5 |
| | User preferences unintentionally deleted | Complete loss of user profile characteristics and fitness goals | a. Database failure | a. Refer to H1-5 | a. INR3 | H1-6 |
| | Database contains duplicate accounts | Inconsistency in user data | a. Account authentication errors | a. Backend validation to ensure no duplicate primary keys | a. INR5 | H1-7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Workout Planning | System does not generate a workout plan according to user profile characteristics | User left without core feature of the app: a generated workout plan | a. AI Algorithm failure | a. Display detailed error message and allow them to try again<br>b. Review data set for more accurate data to train AI model | a. EHR1 | H2-1 |
| Live Workout | User unable to begin workout | User cannot view instructions and guidance for their workout | a. App closes unexpectedly | a. Refer to H5-1a | a. EHR2<br>b. INR4 | H3-1 |
| | Live workout unexpectedly quits | User must stop their workout | a. App closes unexpectedly | a. Display a detailed error message. Store progress as workout progresses so progress is not lost. Using stored progress, allow users to resume workout once system is back up | a. INR6 | H3-2 |
| Workouts | User given inaccurate advice for an exercise | Potential user injury | a. AI model trained on inaccurate data<br>b. Chatbot given too much leeway for workout instruction | a. All data input into the training data set will be extensively reviewed and researched to ensure best fitness practices are followed<br>b. Ensure users are sufficiently warned and provided with guidance for best practices regarding how exercise should feel (e.g. if there is pain, stop) | a. INR7<br>b. INR8 | H4-1 |
| | System does not save workout | Progress tracking unavailable for relevant workout | a. Database failure<br>b. App crashes unexpectedly | a. Refer to H1-4.<br>b. Refer to H5-1a | a. INR4 | H4-2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| General | Application closes unexpectedly | User briefly unable to access app, potential data loss | a. User device loses power<br>b. Server instability<br>c. User device unable to support | a. Store unsaved data locally until application is reopened<br>b. Refer to H5-1a | a. INR4 | H5-1 |
| | User data released without permission | Privacy violation | a. Database failure | a. Implement effective data encryption protocols; update protocols regularly | a. PRR1 | H5-2 |
| | Data unintentionally deleted | Application data lost | a. Database failure | a. Refer to H1-5. | a. INR3 | H5-3 |

Table 2: FMEA table

# 6 Safety and Security Requirements

Requirements written in bold are new requirements that were not included in revision 0 of the SRS, but have been added to mitigate the hazards.

## 6.1 Access Requirements

- ACR1: The app shall enforce strong password restrictions to ensure users are properly protecting their own data.
- ACR2: Users shall authenticate themselves with their credentials securely.
- ACR3: Users will only have access to data and features for which they are authorized.

## 6.2 Integrity Requirements

- INR1: Sensitive data shall be restricted from the users of the app.
- INR2: Data between the app and the server should be encrypted when an API call is made.
- INR3: The system should regularly back up data automatically to prevent data loss in the event of database failures.
- INR4: Unstored data should be stored locally if the data cannot be updated.
- INR5: The system must incorporate backend validation to enforce the uniqueness of primary keys associated with user accounts in the database.
- INR6: The system must have a mechanism to store the user's progress when completing a live workout, allowing them to resume their workout from the point of interruption when the application is reopened.
- INR7: The system should display clear and prominent warnings to users regarding exercise safety.
- INR8: The AI model system should be constantly updated with accurate practices and the data should be reviewed.

### 6.3 Privacy Requirements

- PRR1: Sensitive data should be encrypted both in transit and at rest to protect it from unauthorized access

### 6.4 Error Handling Requirements

- EHR1: The system should have robust error handling that doesn't reveal sensitive system information to users in error messages
- EHR2: The system should include a user feedback mechanism, allowing users to report issues, including unexpected application closures

## 7 Roadmap

### 7.1 During Capstone Timeline

The following requirements will be implemented during the current project timeline

- ACR1
- ACR2
- ACR3
- INR1
- INR2
- INR5
- SECR6
- PRR1
- EHR1

### 7.2 Future Timeline

The following requirements are to be left for future implementation

- INR3
- INR4
- INR6
- INR7
- INR8
- EHR2