Hazard Analysis
4G06 - Software Engineering

Team #9, Housemates
Justin Dang - dangj15
Harris Hamid - hamidh1
Fady Marcos - morocof2
Rizwan Ahsan - ahsanm7
Sheikh Afsar - afsars

Table 1: Revision History

Date	Developer(s)	Change
Oct 20 2023	All	Revision 0

Contents

1 Introduction

1.1 Product

The housemates app will allow for its users to better communicate with their housemates. Additionally the app will have a cost management and chore management system to allow for splitting of chores/costs amongst housemates.

1.2 Document Purpose

The purpose of this document is to identify any potential hazards that could exist in the housemates application and to provide elimination/mitigation strategies to help reduce these risks to manageable levels.

1.3 Scope of Hazard Analysis

The scope of this hazard analysis is covering all of the subsystems of the housemates application. Each subsystem will have its own safety considerations and hazards. This will be done with an FMEA (Failure Mode and Effect Analysis)

1.4 Definition of Hazard

In this document a hazard is defined to be, any feature or property of the housemates application that gives incorrect information to the user or otherwise negatively affects the user experience.

2 System Components

The following sections are descriptions of each of the subsystems that make up the housemates application.

2.1 Task Management System

The task management system of the housemates application will allow users to split and delegate common household tasks to their housemates.

2.2 Bill Management System

The bill management system of the housemates application will allow users to split bills with their housemates.

2.3 Scheduling System

The scheduling system of the housemates application will allow users to schedule events to coordinate with their housemates.

2.4 Account System

The account system of the housemates application will manage and store user data.

3 Critical Assumptions

- The application is running on devices with Android OS
- The devices running the application are in good condition

4 Failure Mode and Effect Analysis

Table 2: Failure Mode and Effect Analysis Table

Ref	Failure Mode	Subsystems	Causes of Failure	Effects of Failure	Recommended Actions	Req
HAZ-1	No Internet	All	User network issues such as weak WiFi signal or not being connected to the internet	a. Users won't be able to access certain features of the application, which can lead to frustration. b. Once users regain internet access, any changes made offline may not sync properly	a. Store data locally on the device to ensure users can access and modify tasks even without an internet connection b. Implement an offline mode that allows users to access certain features of the application locally on their device	IR-1 AR-3
HAZ-2	Malicious or Invalid Input	All	Failure to sanitize user input can open the app to potential security risks like SQL injection or cross-site scripting attacks	a. Malicious actors can inject SQL code into input fields, potentially gaining unauthorized access to the app's database or executing harmful actions b. Incorrectly sanitized input may lead to unintended changes or corruption of data in the database	a. Use proper escaping functions to neutralize special characters in user input to prevent them from being interpreted as code b. Implement strict input validation processes to ensure that user input is free from malicious code	IR-2
HAZ-3	App Closes Unexpectedly	All	Device loses power	Unsaved data lost	Store unsaved data locally and resume progress after app is opened again	IR-1

HAZ-4	Incorrect Task Input	Task Management	Users may accidentally enter incorrect information for tasks, which can lead to inaccurate records or calculations	a. The task management system may contain tasks with incorrect details, leading to confusion about deadlines, priorities, and responsibilities. b. Reports based on inaccurate input can provide misleading insights about task completion	allow users to review and confirm task details before finalizing. This can help catch and correct any mistakes before they become part of the system.	IR-2
HAZ-5	Accidental task deletion by user	Task Management	Users in a hurry may not pay close attention to their actions, potentially leading to accidental deletions	Accidental deletion can result in the permanent loss of important task details	a. Implement a confirmation dialog box that asks users to confirm their intent before permanently deleting a task b. Implement an archiving system that allows users to recover deleted tasks within a certain time frame	IR-2 IR-5
HAZ-6	Users credentials lost	Account	Invalid login credentials Database failure	User cannot access features of the application	Allow users to reset their credentials	AR-2
HAZ-7	Bill Split Incorrectly	Bill Management	a. Miscalculation from bill management system b. It isn't possible to split the bill evenly (e.g. $ 300 split 7 ways)	Bill amount isn't split up evenly	a. Check that bill splits are even b. If even split isn't possible give one of the users the remainder	IR-6
HAZ-8	Bill Split doesn't add up	Bill Management	Miscalculation from Bill Management system	Bill amount from splits doesn't add up to actual bill amount	Check that bill split adds up to actual bill	IR-6
HAZ-9	Round-off error	Bill Management	If data is stored as a float in the database this will cause a 64-bit round off error especially when dealing with multiple transactions.	This will cause all transaction amounts to add up and overestimate the actual bill	When storing bill amount to the database multiply by 100 to convert it to an integer to avoid round-off errors and when retrieving it from the database divide by 100.	IR-2 IR-6

HAZ-10	Access of Information without Authentication	Account	Failure of authentication systems No internet connection	Users allowed unauthorized access	If user is unauthenticated block access to the application until authentication occurs	AR-1 AR-4 PR-1
HAZ-11	Overload of Server	Account	Too many client requests	Client requests in the application will take significantly longer to fulfill	a. Have rate limiting to limit any unusually high amounts of traffic	IR-4
HAZ-12	Schedule Data Lost	Scheduling, Account	Database failure	Scheduled events missed	Automatically back up database at regular intervals	IR-3
HAZ-13	Task Data Lost	Task Management, Account	Database failure	Task information lost	see HAZ-12	IR-3

5 Safety and Security Requirements

5.1 Access Requirements

AR-1: Users must log in to access the features of the application.
AR-2: Users should be able to access their own user data.
AR-3: Users should be able to access the features of the application offline
AR-4: Only system admins should be able to access user data.

5.2 Integrity Requirements

IR-1: The application should store data locally until data can be uploaded.
IR-2: User input should be validated before introduction of data into the database.
IR-3: The database should be backed up daily.
IR-4: Client requests to the server should be rate limited.
IR-5: User deleted data should temporarily be stored.
IR-6: System output should be validated before given to user.

5.3 Privacy Requirements

PR-1: Users should not be able to access other users data.

5.4 Audit Requirements

N/A

5.5 Immunity Requirements

N/A

6 Roadmap

This hazard analysis has discovered new safety and security requirements from the section above that will be added to the SRS. Most of these requirements will be implemented in the final application (i.e. Revision 1), but some may not be due the time constraints of this project.