Hazard Analysis
Housemates

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

Table 1: Revision History

Date	**Developer(s)**	**Change**
Oct 20 2023	All	Revision 0
Apr 4 2024	Sheikh Fardeen Afsar	Revision 1

Contents

1 Introduction 1
1.1 Product 1
1.2 Document Purpose 1
1.3 Scope of Hazard Analysis 1
1.4 Definition of Hazard 1

2 System Components 2
2.1 Task Management System 2
2.2 Bill Management System 2
2.3 Scheduling System 2
2.4 Account System 2

3 Critical Assumptions 2

4 Failure Mode and Effect Analysis 2

5 Safety and Security Requirements 5
5.1 Access Requirements 5
5.2 Integrity Requirements 5
5.3 Privacy Requirements 6
5.4 Error handling Requirements 6
5.5 Audit Requirements 6
5.6 Immunity Requirements 6

6 Roadmap 6
6.1 During Capstone Timeline 6
6.2 Future stretch goals 7

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

This hazard analysis focuses on identifying and mitigating risks associated with the functionality and operation of the Housemates app. The following areas are considered within the scope of this analysis:

- **Software-related hazards** that could impact the app's performance, data integrity, and user interaction.
- **Network-related hazards** that could affect the app's connectivity and online features.
- **User interaction-related hazards** that could lead to unintended app behavior or data loss.

The following areas are considered out-of-scope for this hazard analysis:

- **Device-Related Issues**: Problems stemming from the user's device, such as hardware malfunctions, operating system errors, or issues related to other applications, are outside the scope of this analysis.
- **External Services**: The functionality and availability of third-party services that the app may interact with, but does not control, are not covered by this analysis.
- **User Behavior**: Hazards resulting from user behavior that cannot be controlled or predicted by the app, such as physical damage to the device or misuse of the app, are not included.

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.	Implement an auto-save feature that periodically saves data locally and allow users to set their preferred auto-save frequency.	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.	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
HAZ-14	Offline conflict from multiple users	All	a. Multiple users accessing and modifying schedules, tasks, or payments in offline mode. b. Lack of a system to reconcile changes made by different users once the app goes online.	a. Inconsistent data across user devices. b. User confusion and potential disputes among housemates. c. System failures due to conflicting data entries.	a. Implement a conflict resolution protocol that prompts users to review and resolve discrepancies after reconnecting to the internet. b. Introduce a version control system that tracks changes made by each user and merges them intelligently.	IR-1, AR-3, IR-8
HAZ-15	Integer overflow	Bill Management	Storing large monetary values that exceed the maximum limit of a 32-bit unsigned integer, which is 4,294,967,295.	Incorrect financial calculations and data corruption.	Use suitable data type for monetary values to handle very large integers safely.	ER-1
HAZ-16	Server downtime leading to service unavailability	All	Scheduled maintenance.	Inability for users to access the service.	Develop a communication strategy to inform users of the issue and expected resolution time.	IR-7

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.
IR-7: The application must have a robust mechanism to handle server downtime, ensuring minimal disruption to user activities and maintaining data integrity.
IR-8: The application should resolve or provide a way to resolve conflicts when saving data offline.

5.3 Privacy Requirements

PR-1: Users should not be able to access other users data.
PR-2: The application should receive explicit consent from the users before storing any personal information or allowing usage of the application.

5.4 Error handling Requirements

ER-1: Users should be able to work with large financial numbers. ER-2: Users should be able to

5.5 Audit Requirements

N/A

5.6 Immunity Requirements

N/A

6 Roadmap

6.1 During Capstone Timeline

The following requirements will be completed in Capstone timeline.

- AR-1
- AR-2
- AR-4
- IR-2
- IR-4
- IR-5
- IR-6
- PR-1

6.2 Future stretch goals

The following requirements are future stretch goals to be completed.

- AR-3
- IR-1
- IR-3
- IR-7
- IR-8
- PR-2
- ER-1