Hazard Analysis
Grocery Spending Tracker

Team 1, JARS
Jason Nam
Allan Fang
Ryan Yeh
Sawyer Tang

Table 1: Revision History

Date	Developer(s)	Change
16/10/23	Ryan Yeh	Added List of Tables, List of Figures, and Failure Mode and Effect Analyis
16/10/23	Allan Fang	Added sections 1, 2, 3
17/10/23	Ryan Yeh	Added Critical Assumptions
19/10/23	Sawyer Tang	Initial Version of Safety and Security Requirements
19/10/23	Ryan Yeh	Added Roadmap
01/04/24	Sawyer Tang	Addressed Feedback: updated assumptions for camera availability and web service, updated HA1 and HA2 to include newly added SSR11
04/04/24	Ryan Yeh	Added assumption for user's phone working properly

Contents

1 Introduction 1

2 Scope and Purpose of Hazard Analysis 1

3 System Boundaries and Components 1

4 Critical Assumptions 1

5 Failure Mode and Effect Analysis 2

6 Safety and Security Requirements 5

7 Roadmap 7

List of Tables

1 Revision History i
2 Failure Mode and Effect Analysis Table 2

1 Introduction

This document details the hazards and the associated hazard controls for the Grocery Spending Tracker system to mitigate and eliminate unsafe behaviour. The Grocery Spending Tracker will assist users in making smart grocery decisions to better manage household and grocery expenses. A hazard is defined as some system condition(s) that, together with some environmental condition(s) has the potential to cause loss of some value to stakeholders. A hazard control is a measure to mitigate the hazard.

2 Scope and Purpose of Hazard Analysis

The scope of the document is to identify possible hazards within the system components, the steps to mitigate the hazards, and the resulting safety and security requirements.

3 System Boundaries and Components

The system that this hazard analysis will be conducted on consists of the following components:

- The front-end and back-end components of the application:
  - Authentication
  - Purchase data input (including optical recognition and language models)
  - Nearby alternatives recommendations
  - Purchase history reports
  - Spending objectives
- User mobile device
- The database storing all application data

4 Critical Assumptions

One assumption being made by the team is that, because we are using an existing service to host our back end and database, such as Azure or Amazon Web Service, they will have security protocols in place to mitigate malicious parties. At the current time, all user data will be private and not shared with any party outside of the application.

Another assumption is that the user's phone is working properly in addition to the camera.

5 Failure Mode and Effect Analysis

Table 2: Failure Mode and Effect Analysis Table

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	Req ID	Ref.
Authentication	User is unable to log in	User cannot access their account and application features	a. User entered incorrect credentials	a. Allow users to reset their password b. Two factor authentication for login and password reset.	a. SSR1 b. SSR12	HA1
Authentication	User's account is hacked by a third party	User's data can be read and modified by third party	a. Third-party gains access to the user's account without their permission	a. Refer to HA1-a b. Limit the number of log in attempts a person has for a given time period c. Periodic database backups so that user data can be recovered. d. Require users to create *strong* password. e. Refer to HA1-b	a. SSR1 b. SSR2 c. SSR10 d. SSR11 e. SSR12	HA2

Purchase Data Input	Application improperly reads user's inputted receipt	Inaccurate data is stored to the database affecting application analytics and suggestions	a. OCR interprets certain characters incorrectly from the input b. OCR is unable to read certain words or characters from the input	a. Utilize natural language processing to clean and correct output produced by the OCR b. Prompt user to take another photo if input is unclear c. Allow user to manually input grocery item	a. SSR3 b. SSR4 c. SSR5	HB1
	User is unable to input or take a photo of their receipt	User cannot record their recent shopping data and analytics become outdated	a. Application does not have permissions to access device camera or photo gallery	a. Prompt user to give permissions to the application to access camera and photo gallery	a. SSR6	HB2
Nearby Alternatives Recommendation	Unable to determine user's location	Application is unable to provide nearby alternative recommendations	a. Invalid location data entered by user b. Database failure	a. Utilize front-end and back-end validation on user inputs b. Utilize automatic database backups on a regular basis	a. SSR7 b. SSR8	HC1

	Unable to connect to map/location API	Nearby alternatives recommendation feature fails to work	a. User does not have an internet connection	a. Prompt user to connect to the internet	a. SSR9	HC2
Purchase History Reports	Incorrect data is returned in the reports	User could make incorrect financial decisions based on inaccurate data	a. Database failure b. Problem occurred when writing to database	a. Refer to HC1-b b. Implement validation to check whether data is written correctly	a. SSR8 b. SSR10	HD1
Spending Objectives	Invalid spending objectives input by user	Incorrect or invalid budgeting suggestions provided by the application	a. Invalid data entered by user b. Database failure	a. Refer to HC1-a b. Refer to HC1-b	a. SSR7 b. SSR8	HE1
General	Application unable to access database	Major features in the application will no longer work	a. User does not have an internet connection	a. Refer to HC2-a	a. SSR9	HF1

6 Safety and Security Requirements

SSR1. The system shall allow users to reset their password without logging in and without knowledge of their current password.

Rationale: Users cannot be relied on to remember their login credentials correctly. There must be a method of allowing the user to access their account despite this as well as recover their accounts should a malicious third party gain access.

Associated Hazards: HA1, HA2

SSR2. The system shall limit the number of log in attempts to 5 times within 10 minutes before log in is disabled for a 1 hour cooldown period.

Rationale: Malicious actors may gain access to an account by a brute-force attack. This requirement significantly reduces this possibility.

Associated Hazards: HA2

SSR3. The system shall use natural language processing to reduce the error generated by OCR reading of the receipt.

Rationale: OCR can sometimes return an inaccurate reading of its input. Natural language processing can reduce this by interpreting the reading using its model rather than its literal reading.

Associated Hazards: HB1

SSR4. The system shall prompt the user to retake a photo if the receipt reading is unclear.

Rationale: OCR will return incorrect data to the rest of the system if the photo is unclear. Thus requesting the user to retake the photo can mitigate this issue.

Associated Hazards: HB1

SSR5. The system shall allow the user to manually input grocery items.

Rationale: Should the OCR and language model not read or recognize an item properly, the user can eliminate this error state by manually reviewing and inputting their items.

Associated Hazards: HB1

SSR6. The system shall prompt the user to grant system access to the device camera and the photo gallery.

Rationale: If the application does not have camera access, it cannot take a photo. The prompt will notify the user that they must grant access before the application can take or import a photo.

Associated Hazards: HB2

SSR7. The system shall perform data validation on both front-end and back-end for user inputs.

Rationale: If data between modules is incorrect, a type/correctness validation can eliminate or mitigate the risk of unpredictable behaviour or error.

Associated Hazards: HC1, HE1

SSR8. The system shall perform database backups on a regular basis.

Rationale: If the database has a failure and loses data or is offline, the system will be unable to perform some of its functions. Backing up the database will ensure swift recovery and limited data loss.

Associated Hazards: HC1, HD1, HE1

SSR9. The system shall prompt the user to connect to the internet if the system is not connected to the internet.

Rationale: The system will not function correctly without internet connection. Prompting the user to obtain internet connection will notify that user what the problem is and how they might address it.

Associated Hazards: HC2, HF1

SSR10. The system shall validate that the information in the database is correct.

Rationale: If there is a mistake in an operation on the database, it can provide the user with false insights. By validating the database after it is augmented, the error state can be mitigated.

Associated Hazards: HD1

SSR11. The system shall require users to create a *strong* password when making their account or changing their password. (ie. includes at least one special char and one number).

Rationale: Numbers and special characters make it more difficult for malicious actors to obtain a user's password.

Associated Hazards: HA2

SSR12. The system shall allow users to use the users email as a two-factor authentication. The system will send the user a verification code to input both after login and when attempting to reset the users password.

Rationale: Users should have the option to enhance the security of their account in the case their password is compromised.

Associated Hazards: HA1, HA2

7 Roadmap

Many Safety and Security Requirements were identified however due to time constraints, not all of them will be addressed by the team for the Revision 1 version. The requirements that the team will be prioritizing are SSR3, SSR5, SSR6, and SSR9. Should the team find themselves with extra time before this deadline, other requirements may be considered however these four would be essential for the core application functionality. In general, the remaining requirements will be implemented at a future date.