Hazard Analysis
Software Eng 4G06

Team 2, Parnas' Pals
William Lee
Jared Bentvelsen
Bassel Rezkalla
Yuvraj Randhawa
Dimitri Tsampiras
Matthew McCracken

Table 1: Revision History

Date	**Developer(s)**	**Change**
Date1	Name(s)	Description of changes
Date2	Name(s)	Description of changes
...	...	...

Contents

1 Introduction

The purpose of this document is to identify the components of Olympian and its dependencies that could represent potential risks for Olympian's stakeholders. This document will analyze the risk levels of potentially hazardous components and their associated failures, as well as recommend actions which can be taken to eliminate the resulting risks or mitigate them to an acceptable level.

1.1 Definition of a Hazard

For Olympian's purposes (and throughout this document), a hazard will be defined as any condition or event which can lead to a state that is likely to negatively affect Olympian's stakeholders.

2 Scope and Purpose of Hazard Analysis

3 System Boundaries and Components

4 Critical Assumptions

- The user is assumed to have the Olympian application downloaded.
- The user's mobile device is assumed to have internet access.
- The user is assumed to have basic mobile device skills such as tapping the screen and swiping.

[These assumptions that are made about the software or system. You should minimize the number of assumptions that remove potential hazards. For instance, you could assume a part will never fail, but it is generally better to include this potential failure mode. —SS]

5 Failure Mode and Effect Analysis

5.1 Hazards Out of Scope

Hardware Failure

5.2 Failure Modes & Effects Analysis Table

Failure Modes & Effect Analysis						
Component	Failure Modes	Effects Of Failure	Causes Of Failure	Recommended Action	SR	Ref.
User Login & Authentication	User cannot log in to application	User cannot utilize site functionality	a. User uses incorrect login credentials.	Reset user's credentials.		
User Private Data Access	Data that is meant to be kept private is displayed publicly	Users privacy is breached and sensitive data is released	a. Users privacy settings are incorrectly stored. b. Malicious third party gains access to user data.	User data will be backed up daily to avoid error. Utilize stringent AWS admin permissions.		
User Visual Interface						
Workout Suggestion Algorithm						
Application Server						
Database						

6 Safety and Security Requirements

[Newly discovered requirements. These should also be added to the SRS. (A rationale design process how and why to fake it.) —SS]

6.1 Access Requirements

ACR1: The application must not display other users private details to the user.

ACR2: Only the developers and system administrators will be able to access all user details except their passwords.

6.2 Integrity Requirements

IR1: Passwords must be encrypted with SHA-256 when stored.

IR2: User data will not be modified void of user permission.

IR3: User data will be automatically backed up to the database upon connection to the internet.

IR4: User data will be stored locally.

6.3 Privacy Requirements

PRR1: The application must use OAuth protocols to verify communication between the client and server.

PRR2: The application will ensure users are aware of data collection practices before collecting any data from them.

PRR3: The application will communicate any changes to the privacy policy with the users.

6.4 Audit Requirements

ADR1: Data will be stored in a secure database. When data is deleted or edited a record of this data will be kept for up to 30 days.

6.5 Immunity Requirements

- N/A

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]

Based on the safety requirements listed above, the table below displays which of the requirements are planned for the current timeline of the project and those that planned implementations for the future.

Planned	Future
ACR1	ADR1
ACR2	
IR1	
IR2	
IR3	
IR4	
PRR1	
PR2	
PR3	