Hazard Analysis
REVITALIZE

Team 13, REVITALIZE
Bill Nguyen
Syed Bokhari
Hasan Kibria
Youssef Dahab
Logan Brown
Mahmoud Anklis

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 15th, 2022	Bill Nguyen	FMEA
...	...	...

Contents

[You are free to modify this template. —SS]

1 Introduction

[You can include your definition of what a hazard is here. —SS]

2 Scope and Purpose of Hazard Analysis

3 System Boundaries and Components

4 Critical Assumptions

[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

The next pages will show the full failure mode and effect analysis (FMEA) for REVITALIZE:

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref
Login	Login failed with invalid credentials	User cannot login and use/view app	Invalid login credentials	Reset user's credentials		H1-1
	Login failed with valid credentials	User cannot login and use/view app	Account locked temporarily Credentials are expired Mismatch of credentials in user input and database	Check if account is locked and if appropriate unlock account Wait for account to be unlocked Check if the credentials inputted by user matches credentials in database		H1-2
	Unauthorized login by invalid user	Invalid user can login and use/view/edit app where they do not have permission to do so	Illegal access to credentials that are gathered from potential tactics such as phishing, leaks, hackages etc.	Rollback changes made by invalid user to previous state Restrict access to invalid user and fix account permissions Flag issues that can be related to phishing, leaks, hackages etc.		H1-3
	Login database/server down	Percentage of users ranging from 0-100% cannot access app	All technologies/services related to login (ex. Backend services, database) is down	Have constant checks of overall health of related services Have alarms to inform when these issues have arised		H1-4
User Account	Backend services are compromised	Potential loss of user data	Database services are compromised/manipulated Failures such as memory errors, service crashes etc.	Have alarm and monitor for potential compromises and make the appropriate changes/rollbacks when needed		H2-1
	Spam accounts	Can cause an unnecessary usage and an excess of users that will take available resources from actual users	DDOS/Cyber attacks on app usually from automated programs	Adding potential CAPTCHAs and validation checks to prove that this is real user and not a "bot"		H2-2
Database	Data is deleted	Percentage of data ranging from 0-100% will be lost	Failures related to the database Cyber attacks Invalid access to database services	Have backup databases Rollback changes to previous state where data was not deleted Have preventive measures to make sure data is not deleted unintentionally		H3-1
	Unable to use database	Users and all stakeholders are unable to use app data	Refer to H3-1	Display error message that is detailed and message that all users can understand Give potential timeline to user of when issue can be fixed Have preventive measures to avoid this issue		H3-2

Figure 1: Part 1 of FMEA

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]

7 Roadmap

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