Hazard Analysis
Course Buddy

Team #5, Overwatch League
Jingyao, Qin
Qianni, Wang
Qiang, Gao
Chenwei, Song
Shuting, Shi

Table 1: Revision History

Date	**Developer(s)**	**Change**
2023/10/19	Chenwei Song, Qiang Gao	Initial draft of the document
...	...	...
...	...	...

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

Design Function	**Failure Modes**	**Effects of Failure**	**Causes of Failure**	**Detection**	**Recommended Action**	**SR**
User Registration	Username not accepted	Inability to access the tool	Username already exists	Authentication system would check username uniqueness	Notify the user to choose another username	SR1 SR2 SR4 SR6
User Login	Login failure	Denied access	Password mismatch	Authentication system would check username and password match	Provide password recovery	SR1 SR2 SR5 SR4 SR6 SR7
Task Generation	No tasks generated	Disorganized schedule	PDF extraction module not recognizing certain tasks	User feedback	Systematic bug fixes	FR16 PAR1
Task Prioritization	Incorrect prioritization	Mismanaged time	Algorithm error	User feedback	Refine prioritization algorithm	SR3 FR17 PAR1
Progress Visualization	Inaccurate visuals	Misunderstanding of progress	Progress data not updated with user feedback	Regression tests	Make sure visualization module uses updated data	SR3 FR20 OER3
Connected Learning	Connection issues	Isolation in learning	Network instability	Connectivity checks	Run a connectivity check when the user attempts connected learning	SLR1
Export to Other Calendars	Export failure	Disconnected schedules	Compatibility issues	User feedback	Enhance compatibility layers	SR5 SR3 AR1
Estimate Task Duration	Incorrect estimates	Misallocated time for tasks	Algorithm inaccuracies	User feedback	Refine estimation algorithms	FR14

6 Safety and Security Requirements

- **SR1: Data Encryption**
  - **Description:** Ensure data encryption during data transfers to prevent unauthorized access.
  - **Fit Criteria:** Data being transferred should be encrypted using industry-standard algorithms, with no plain-text data leaks detected.
  - **Function to Fulfill:** Implement encryption protocols in the data transfer modules.
- **SR2: Encrypted Data Storage**
  - **Description:** Store user data in a hashed or encrypted format to prevent direct access.
  - **Fit Criteria:** No user data should be retrievable in plain text from the storage systems.
  - **Function to Fulfill:** Use encryption/hashing mechanisms in the data storage systems.
- **SR3: Audit Log Maintenance**
  - **Description:** Maintain an audit log of all activities within the application for traceability and accountability.
  - **Fit Criteria:** All user and system activities should be logged with time stamps and relevant meta-data.
  - **Function to Fulfill:** Integrate an activity logger within the application framework.
- **SR4: Role-based Access Control**
  - **Description:** Have a strict role-based access control to prevent unauthorized data manipulation.
  - **Fit Criteria:** Different user roles should have differing access levels, with no unauthorized data access incidents.
  - **Function to Fulfill:** Implement role-based access control mechanisms in the user management module.
- **SR5: Security Patches and Updates**
  - **Description:** Provide regular security patches and updates to the software to rectify known vulnerabilities.
  - **Fit Criteria:** No known vulnerability should persist in the system for more than a month without a patch.
  - **Function to Fulfill:**Establish a dedicated security updates team.
- **SR6: Attack Prevention**
  - **Description:** The system should protect authentication data from brute force attacks.
  - **Fit Criteria:** Restriction after a certain number of failed login attempts; option for the user to unlock account via email or phone.
  - **Function to Fulfill:**Implement rate-limiting to prevent brute force attacks.

- **SR7: Password Recovery**
  - **Description:** The system should provide a mechanism for users to retrieve their passwords in case they forget them.
  - **Fit Criteria:** A user who has forgotten their password should be able to receive a password reset link via their registered email. This link should expire after a certain duration.
  - **Function to Fulfill:**Implement a password recovery module that generates and sends a time-bound password reset link to the user's registered email.

7 Roadmap

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