**Risk Assessment and Management Plan (RMP)**

**Version 3.0**

**1. Introduction**

The Risk Assessment and Management Plan (RMP) is designed to identify and address potential risks that could affect our project's progression negatively. By identifying risks based on user stories, assessing their likelihood and severity, and implementing appropriate mitigation strategies, we aim to minimize their impact as much as possible.

**2. Understanding used Metrics**

It is vital to understand how we define a risk and how we quantify it. For instance, **we define risk as any event that might disrupt team efficiency, particularly regarding manpower.**. By this, we mean that anything that may pose as a nuisance to the entirety of the team is considered a risk. Given that manpower can be disrupted in several ways, we have identified and categorized types of risks below:

* **Technical Risks:** Include issues related to technology performance, security, and compatibility.
* **Organizational Risks:** Encompass challenges related to resources, budget management, scheduling, and communication.

Upon understanding the type of risk we deal with, analyzing the risk is the next step. For this, there are two metrics to consider: probability and impact.

* **Probability**: Assessed as low, medium, or high based on past experiences and patterns in software development projects.
* **Impact**: Evaluated based on its effect on performance, schedule, and cost, with severity rated as low, medium, or high. We have disclosed that an impact of a risk can be affected in 3 ways:
  + **Performance**: technical, personal experience, documentation
  + **Schedule**: delays, task dependencies, inadequate times estimates for tasks
  + **Cost**: respecting budget

In order to quantify impact, we take several factors into consideration, and we scaled the level of impact a risk has based on the ratings below:

* + **Low**: has no effect on the user, can be reversed quickly, is part of the process (e.g. redesigning)
  + **Medium**: needs reworking, leads to poor app performance (e.g. slow loading times)
  + **High**: Blocks other user stories/tasks, needs a lot of reworking, leads to data loss, leads to security breach.

The probability and the impact of a risk can be identified through the usage of a risk matrix as we have done so in Section 4.

**3. Risk Assessment and Management Plan**

Given that we have identified 2 types of risks that can affect manpower, our focus on risk assessment and mitigation will be put on those as follows.

Regarding technical risks, problems such as compatibility issues, scalability challenges and data breaches are all possible. Acknowledging these risks as well as being able to mitigate them is vital in RMP. For instance, to overcome such technical risks once apparent, regular maintenance and updates to the application will address vulnerabilities and improve performance. In addition, implementing security measures such as encryption, firewalls and access controls will help protect against unwarranted access. Thorough testing throughout will also help in mitigating technical risks before deployment.

Regarding organizational risks, it’s important to recognize and consider issues such as key personnel dependency and competing priorities. To mitigate organizational risks, establishing clear channels of communication, fostering engagement amongst all team members, diversification of dependencies and resource planning are all crucial mitigations to ensure alignment with the project objectives and minimization of organizational risks.

As such, depending on the type of risk, be it technical or organizational, the according mitigation plans are set in place to ensure that risks are well considered for resolution.

Regardless of the type of manpower encountered, both will follow the same risk assessment plan. This can be broken down into 5 steps as follows:

1. **Risk Identification:** The purpose of risk identification is to create a list of potential risks, covering a range of categories. By identifying risks early on, we can proactively address them and minimize them.
2. **Risk Analysis:** The purpose of risk analysis is to calculate the risk exposure for each risk. That is, we analyze the probability of each risk occurring and estimate its impact, all of which are based on the way we quantified both probability and impact.
3. **Risk Prioritization:** The purpose of risk prioritization is to consider the results gathered from analysis and to prioritize the risks according to their risk exposure (probability and impact). Prioritizing risks allows us to focus our efforts and resources on addressing the most critical threats.
4. **Risk Planning and Resolution:** The purpose of risk planning is to identify appropriate risk responses such as avoidance, mitigation, acceptance, or transfer and to implement such strategies. Risk planning ensures that we are quipped to respond effectively to adverse events and minimize their impact throughout the course of the project.
5. **Risk Monitoring:** The purpose of risk monitoring is to keep track of risk changes and assessing the effectiveness of risk management activities defined in the previous step. Risk monitoring involves communicating risk status to relevant stakeholders and enables us to adapt to ongoing threats.

**4. Risk Matrix**

The categorization of user stories can be represented in figure 1:

| Impact  Probability | Low | Medium | High |
| --- | --- | --- | --- |
| Low | CN-25, CN-130, | CN-37, CN-32, CN-57, CN-56, CN-55 | CN-2, CN-15, CN-31, CN-66, CN-67, CN-132, CN-139, CN-129 |
| Medium | CN-149 | CN-29, CN-53, CN-128 | CN-97 |
| High | CN-87 |  | CN-65 |

Figure 1: Risk management chart

| Risk ID | Risk Type and Description | Risk Score | Resolved in Sprint | Strategy and Effectiveness |
| --- | --- | --- | --- | --- |
| CN-2 | Technical: Inadequate security measures can lead to data leaks | * Probability: Low * Impact: High * Overall: Medium | 1 | Avoid: Incorporate secure measures against security threats (HTTPS, input validation) |
| CN-15 | Technical: Unprotected routes in backend can lead unauthorized access | * Probability: Low * Impact: High * Overall: Medium | 1 | Avoid: Implement route protection mechanisms and regularly review its configurations |
| CN-37 | Technical: Inefficient handling of storage of profile pictures can lead to performance issues | * Probability: Low * Impact: Medium * Overall: Low | 1 | Mitigate: Implement optimized storage solutions for profile pictures |
| CN-29 | Organizational (Schedule): Ambiguous activity diagrams may result in delays due to workflow misunderstanding | * Probability:Medium * Impact: Medium * Overall: Medium | 1 | Mitigate: Collaborate with all team members to ensure everyone agrees on a consistent design that fits the overall requirements |
| CN-25 | Organizational (Schedule): Poorly designed component diagrams can lead to delays due to  misunderstanding the system architecture | * Probability: Low * Impact: Low * Overall: Low | 1 | Accept: Later design choices related to component diagrams will result in minimal cons as component driven features can always be updated internally. |
| CN-32 | Organizational (Management): Unclear vision in product statement can lead to misalignment among team members | * Probability: Low * Impact: Medium * Overall: Low | 1 | Avoid: Given that a baseline already exists in terms of the product vision, misinterpretations can easily be avoided through communication effectively as a team |
| CN-31 | Technical: Inadequate security measures could allow a user to falsely modify another user’s profile info. | * Probability: Low * Impact: Hight * Overall: Medium | 2 | Avoid: Ensure that only logged in users with valid token can modify their own profile |
| CN-53 | Technical: If a manager has many properties to manage, inadequate displaying of the properties may lead to incorrect managing | * Probability: Medium * Impact: Medium * Overall: Medium | 2 | Avoid: User a general Data Table component that can handle a lot of information and many actions. |
| CN-67 | Technical: Unprotected routes in backend can lead to unauthorized access | * Probability: Low * Impact: High * Overall: Medium | 2 | Avoid: Implement route protection mechanisms and regularly review its configurations |
| CN-55 | Design: In-adherence to the design could lead to submitting incorrect information to the form and corrupt the database. | * Probability: Low * Impact: Medium * Overall: low | 2 | Avoid: Adhere to the UX designs and follow the class diagram to ensure all the necessary data are passed. |
| CN-56 | Design: In-adherence to the design could lead to submitting incorrect information to the form and corrupt the database. | * Probability: Low * Impact: Medium * Overall: low | 2 | Avoid: Adhere to the UX designs and follow the class diagram to ensure all the necessary data are passed. |
| CN-57 | Design: In-adherence to the design could lead to submitting incorrect information to the form and corrupt the database. | * Probability: Low * Impact: Medium * Overall: low | 2 | Avoid: Adhere to the UX designs and follow the class diagram to ensure all the necessary data are passed. |
| CN-65 | Organizational (Schedule): Due to the complexity of the user story, it is a blocker for other user stories (CN-66 and CN-67). Delays in this user story delay the entire project | * Probability: High * Impact: High * Overall: High | 2 | Mitigation: divide the story down into smaller tasks that can be done simultaneously and divide them among members to ensure faster development |
| CN-66 | Technical: Unprotected routes in backend can lead to unauthorized access | * Probability: Low * Impact: High * Overall: Medium | 2 | Avoid: Implement route protection mechanisms and regularly review its configurations |
| CN-97 | Organizational (Schedule): Since this is the first main user story for the mobile app, delays in would leave to delays in subsequent stories. | * Probability: Medium * Impact: High * Overall: High | 2 | Mitigate: Divide the user story on multiple subtasks that could lead to smoother development. |
| CN-132 | Technical: Since we now deal with financial data, data breaches and unauthorized access are a lot more concerning | * Probability: Low * Impact: High * Overall: Medium | 3 | Avoid: Ensure proper security measures are in place to promote secure financial measures |
| CN-130 | Technical: If the backend calculations are not done correctly, this can lead to inaccurate estimates for parking price | * Probability: Low * Impact: Low * Overall: Low | 3 | Avoid: Ensure adequate testing measures are in place to generate accurate parking fees |
| CN-128 | Design: Given that there is a lot more data involved with the property financial management, user interface design may be inconsistent with all other designs, leading to a poor user experience for employees | * Probability: Medium * Impact: Medium * Overall: Medium | 3 | Mitigate: Reference other Figma designs from other pages to ensure adequate consistency in terms of UI. |
| CN-139 | Technical: a large number of condos belonging to an owner may lead to scalability issues, causing performance degradations | * Probability: Low * Impact: High * Overall: Medium | 3 | Avoid: Ensure frontend system follows modern procedures form a service standpoint so that all condos can be shown on screen. |
| CN-149 | Design: Discrepancies in UI design between the web and mobile app can result difficult mobile implementation | * Probability: Medium * Impact: Low * Overall: Low | 3 | Accept: Different designs from the mobile and web app are to be expected. To ensure seamless mobile development, accurate Figma design should be well referenced. |
| CN-87 | Technical: Inexperience in mobile development leads to difficulties in carrying out the task | * Probability: High * Impact: Low * Overall: Medium | 3 | Accept: Ensure that Mobile developers first learn the basics and how it differs from web development. |

| CN-129 | Technical: Poor handling in the backend can result in retrieving employees that may not belong to an owner’s company. | * Probability: Low * Impact: High * Overall: Medium | 3 | Avoid: Use multiple test cases to ensure backend logic is consistent with the feature’s requirements. |
| --- | --- | --- | --- | --- |