**Risk Management Plan**

The Risk Management Plan (RMP) details the elements of risk to a project.

| **Project Name:** | AutoMart |
| --- | --- |
| **Project Number:** |  |
| **Date:** | 01/03/2023 |
| **Prepared by:** | Emiliano Cabrera, developer |
| **Project Ownership:** | Gilberto Echeverría Furió |

**Project Contacts**

|  | **Name** | **Title/Position** | **Phone** | **Email** |
| --- | --- | --- | --- | --- |
| Primary | Diego Corrales Pinedo | Developer |  | A01781631@tec.mx |
| Other | Andrew Dunkerley Vera | Developer |  | A01025076@tec.mx |
| Other | Emiliano Cabrera Ruiz | Developer |  | A01015453@tec.mx |
| Other | Andrés Briseño Celada | Developer |  | A01352283@tec.mx |
| Other | Do Hyun Nam | Developer |  | A01025276@tec.mx |

**Version Control**

*Add new rows to the table as necessary.*

| **Version Number:** | 1.0 |
| --- | --- |
| **Released:** | 01/03/2023 |
| **Reason/Comments:** | First version of the Risk Management Plan. |

Approved By: Date:

**Risk Assessment and Management Table**

*This table can be adapted to fit the circumstances of individual projects, including non-IT projects.*

*The project manager should retain the category headings in the RMP template, but change, add and delete table entries within those categories to customize the template to fit the specific project being addressed: project management risks, security risks, resource risks, client risks, technical risks, other risks.*

*Use the algorithm at the end to determine the priority of risk.*

| **Risk** | **Description** | **Likelihood[[1]](#footnote-0)** | **Consequences[[2]](#footnote-1)** | **\*Priority of risk [[3]](#footnote-2)**  \*\*Use algorithm | **Owner of the Risk** | **Control Strategies:**  **Mitigate or Accept** | **Proposed Containment Actions** | **Contingency Plan?**  **(Yes, No)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project Management Risks** | | | | | | | | |
| Inadequate project definition | Unclear or wrong requirements, scope or project plan. | Unlikely | Major | Significant | Developers | Mitigate | Establish consistent communication with clients and get validation from clients and advisers after Requirement Phase. | Yes |
| Unrealistic time frames | Deadlines established in unrealistic dates. | Likely | Moderate | Significant | Developers | Mitigate | Prioritize activities based on which cannot be delayed, according to the Critical Route. | Yes |
| Project plan deficient | Project plan lacks clarity and specificity. | Unlikely | Major | Significant | Developers | Mitigate | Establish consistent communication with clients and get validation from clients and advisers after Requirement Phase. | Yes |
| Scope creep | Constantly adding features and functions to the base plan during development. | Rare | Moderate | Moderate | Developers and clients | Mitigate | Define and validate project scope in the Project Definition. | Yes |
| Lack of communication | Not enough communication between clients, developers and advisers. | Likely | Catastrophic | Very high | Developers and clients | Mitigate | Get client contact information and establish consistent communication between clients and developers. | Yes |
| Lack of proper documentation | Missing documents, inconsistent or incorrect information. | Likely | Major | High | Developers, advisers and clients | Mitigate | Request weekly feedback from Project Management advisers on the created documentation. | Yes |
| **Security Risks** | | | | | | | | |
| Security requirements met | Security requirements are properly defined to provide sufficient information security and these requirements are met in the implementation. | Unlikely | Catastrophic | High | Developers and advisers | Mitigate | Get validation from clients and advisers on security requirements after Requirement Phase and validation on implementation after Development Phase. | Yes |
| Accuracy and integrity of data and information | Information is correct and consistent across the system. No unauthorized modification of information is allowed. | Unlikely | Catastrophic | High | Developers and clients | Mitigate | Use industry-standard encryption/hashing algorithms and methodologies. Access to the application is session-based. There are different levels of access that are only assigned by administrators. | Yes |
| Principle of least privilege is followed | Users are only given access to the necessary information to do their jobs. | Rare | Catastrophic | Significant | Developers and clients | Mitigate | There are different levels of access that are only assigned by administrators. | Yes |
| Human vulnerabilities | Improper management of the system, such as not following the principle of least privilege when assigning access levels. Weak passwords. Vulnerability to social engineering. | Likely | Catastrophic | Very high | Developers, advisers and clients | Mitigate | There are different levels of access that are only assigned by administrators. Documentation on usage will be provided by developers to the client for them to distribute. An intuitive design will also be integrated for non-administrative users. |  |
| **Resource Risks** | | | | | | | | |
| Staff turnover | Development team attendance to class and meetings. | Almost certain | Minor | Significant | Developers | Mitigate | Daily SCRUM meetings. | No |
| Unclear roles and responsibilities | Members of the development team not knowing what their responsibilities are. | Moderate | Moderate | Significant | Developers | Mitigate | Establish roles for each developer in the first week. Monitor and update duties in accordance to development schedule. | Yes |
| Level of project team expertise | How much experience and know-how the development team has in secure webapp development. | Moderate | Moderate | Significant | Developers and advisers | Mitigate | Attend class and ask advisers for help when necessary. Get validation from advisers at the end of each phase. | Yes |
| Insufficient funding | Lack of monetary resources for development. Free software usage is encouraged and a mandatory alternative with such elements will be proposed. | Rare | Insignificant | Trivial | Developers | Accept |  | No |
| Insufficient staff | Not enough members of the development team or advisers to efficiently develop the application. | Rare | Major | Significant | Developers | Accept |  | No |
| Insufficient total time | Not enough total time assigned to develop the project from beginning to end. | Rare | Major | Significant | Developers | Accept |  | No |
| **Client Risks** | | | | | | | | |
| Inadequate business requirements | The client’s requests are unrealistic considering their resources. | Rare | Major | Significant | Developers, advisers and clients | Mitigate | Constant client meetings in order to ascertain and narrow requirements to a doable scope. This also includes consulting experts and interested parties to satisfy the needs of the client while keeping an understanding of what is capable of being delivered. | Yes |
| Dissatisfaction with product in acceptance tests | The client does not approve of the application in acceptance tests meant to validate progress. | Moderate | Major | High | Developers | Mitigate | Establish consistent communication with clients via email and get validation from clients and advisers after Requirement Phase. | Yes |
| Training of clients/users | Clients must be trained on how to use the system. | Almost certain | Minor | Significant | Developers, advisers and clients | Mitigate | A developer guide will be provided to the clients by the developers, as well as a user guide to complement future implementation and deployment. Relevant contact details will also be provided in case of any unclear instructions within the manuals. | Yes |
| **Technical Risks** | | | | | | | | |
| Procurement issues, including tendering | Problems obtaining necessary resources for development. This is not a concern for this project as all resources are either free or procured by Tec de Monterrey. | Rare | Insignificant | Trivial | Developers, advisers | Accept |  | No |
| Development hardware inadequate | The hardware used by the development team is not powerful enough to create the application. | Rare | Moderate | Moderate | Developers | Accept |  | No |
| Software unavailable | There is no adequate free software for development of the application. | Rare | Minor | Trivial | Developers | Accept |  | No |
| Technical problems | Accidental loss of development resources, such as broken computers. | Unlikely | Major | Significant | Developers | Mitigate | The latest version of the project will be uploaded in an online repository available to all developers. Documentation is stored in Google Drive. | Yes |
| **Other Risks** | | | | | | | | |
| Interdependencies with other systems | The application depending on other systems to function correctly. Critical parts of the program will be replaced as to give full management to the client after delivery, so there is no need for concern over this event. | Rare | Insignificant | Trivial | Developers, clients | Accept |  | No |
| Level of ongoing support | How much support will be provided to the clients post-installation. | Almost certain | Moderate | High | Developers, advisers, clients | Mitigate | Both a developer guide and user guide will be provided to the clients by the developers for to be able to deploy the project. Relevant contact details will also be provided in case of any unclear instructions within the manuals. | Yes |

1 Likelihood = Almost Certain, Likely, Moderate, Unlikely or Rare

2 Consequences = Insignificant, Minor, Moderate, Major or Catastrophic

3 Priority of risk = Very High, High, Significant, Moderate, Low or Trivia

**\*\*Algorithm for Determining Prioritization of Risk**

| **Likelihood** | **Consequences** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| **Almost Certain** | **Significant** | **Significant** | **High** | **Very high** | **Very high** |
| **Likely** | **Moderate** | **Significant** | **Significant** | **High** | **Very high** |
| **Moderate** | **Low** | **Moderate** | **Significant** | **High** | **High** |
| **Unlikely** | **Low** | **Low** | **Moderate** | **Significant** | **High** |
| **Rare** | **Trivial** | **Trivial** | **Moderate** | **Significant** | **Significant** |

1. Likelihood = Almost Certain, Likely, Moderate, Unlikely or Rare [↑](#footnote-ref-0)
2. Consequences = Insignificant, Minor, Moderate, Major or Catastrophic [↑](#footnote-ref-1)
3. Priority of risk = Very High, High, Significant, Moderate, Low or Trivial [↑](#footnote-ref-2)