Portant - Protecting Sensitive Data from Multiple Sources

Project Plan and Quality Manual

COMP3850 – Computing Industry Project

Group 37 – Edward Morris, Bradley Anderson, Socheat Chhun, Arshita Jayral, Md Mehedy Hasan, Jarrod Adair,

Contents

1. Table of Revisions

Version	Publish Date	Change Description/Features
1.01 Project Plan and Quality Manual	04/01/2021	Submission of version 1 with updated Project plan and Quality Manual
1.02 Project Plan and Quality Manual	23/04/2021	Revision history table added and updated. Handover requirements section created.
1.03 Project Plan and Quality Manual	24/04/2021	Details added in section 3 with updated resources allocated

2. Purpose

The purpose of this project plan is to outline the project timeline and define the scope of the project. This is in addition to stating the risks of development, resources available and the items and documentation that will be delivered by the project's conclusion. These will all be laid out in this document to ensure that all stakeholders involved will be on the same page on all aspects of the project plan.

In addition to the above, the quality manual will detail the quality management practices that will be used in the project, the standards set, how they will be met and how they will be checked to see that they have been fulfilled. Change management will detail how changes will be tracked and managed as the project moves along. The review, auditing, and testing standards will be described and how they be used to fulfil the quality standard that have been set. Finally, the communications channels and how the group will proceed with conflict resolution should it arise will be discussed.

The scope of the project involves the creation of a secure method of requesting and delivering information via emails, forms, and Google Docs. As it stands, the existing product can shift large amounts of information between documents and lay them out in a clean and easy to read format so that leaves the focus of the project on developing the security measures for transit and storage.

3. Risk Management

3.1. Risk Matrix

The risk matrix metrics are as follows:

Likelihood

1. Rare – An event or risk that is highly unlikely to happen within the timeframe of the project. Would only happen once during the project if it were to occur. A 1 in 1000 chance of happening.
2. Unlikely – An event or risk that would come up at most twice during the project but still be a relatively infrequent occurrence. A 1 in 250 chance of happening.
3. Possible – An event or risk that has a moderate chance of occurring on any given week. A 1 in 50 chance of happening.

4. Likely – An event or risk that will probably occur over the course of the project, a 1 in 10 chance of happening.
5. Almost Certain – An event or risk that is mostly guaranteed to happen in any given week. A 1 in 2 chance of happening.

Impact

1. Insignificant – A risk or event that will leave the project relatively unaffected. Sets back the project an hour or so at most.
2. Low – A risk or event that may impact the work on or proceedings of the project for around a few hours or so. May involve a minor loss of progress.
3. Moderate – A risk or event that may impact work on the project for a day or more. Some loss of progress involved.
4. High – A risk or event that may impact work on the project for a week or more. A significant loss of progress may be involved.
5. Catastrophic – A risk that may completely derail the project and may require a complete restart or rework of the project. A significant to complete loss of progress involved.

Risk Level

1. Low – Requires analysis and monitoring to ensure the risk does not get too great. Acceptable risk
2. Medium – Requires more analysis and a mitigation strategy/fallback. Acceptable risk with proper preparations
3. High – Requires more thorough analysis into mitigation/prevention of risk. Action will be necessary to ensure that it does not affect the project.
4. Extreme - Requires thorough examination and evaluation of risks and mitigation measures. Immediate action necessary.

	Impact				
Likelihood	**1 – Insignificant**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Catastrophic**
1 – Rare	Low	Low	Low	Medium	High
2 - Unlikely	Low	Low	Medium	Medium	High
3 - Possible	Low	Medium	Medium	High	High
4 - Likely	Low	Medium	High	High	Extreme
5 – Almost Certain	Medium	Medium	High	Extreme	Extreme

3.2. Risks

3.2.1. Loss of Project

Description: The project files and documentation are partially or completely lost due to destruction/corruption of storage devices. This could be for any reason be it natural disaster, hardware failure or accidental or intentional destruction of storage media.

Probability: 1 – Complete loss of a project should be a very rare occurrence.

Impact: 5 – Depending on how much/what is lost could set the project back several weeks or even require restarting it.

Risk Level: High

Mitigation: The project and its documentation will be kept on cloud services such as GitHub and OneDrive. This is to ensure that all group members copies are up to date as well as ensuring that all files can be accessed from any machine should anything happen to a local device.

3.2.2. Failure of Fulfilling Proper Requirements

Description: The delivered requirements and documentation does not meet the sponsor's requirements due to a breakdown in communication between group members, the sponsor or both. Could also come about with over scoping or the addition of too many requirements.

Probability: 3 – Is more likely the less contact we have with the sponsor and the more the group tries to scope requirements on their own.

Impact: 3 – Could result in a completely different project if requirements were not well defined and never clarified.

Risk Level: Moderate

Mitigation: Weekly meetings with the team and with the sponsor will keep everyone up to date and will allow the sponsor to check in on progress and clarify requirements to ensure development is on the right track.

3.2.3. Failure to Integrate with Existing Product

Description: The delivered product does not integrate with the sponsor's existing product/s due to lack of testing or failure to consider the original product in the design, development, or testing.

Probability: 3 – Would occur only with improper testing since this product uses the same API and transport method of the original product as a base.

Impact: 2 – Not a big problem since the developed application will be very similar in function to Portant's original product.

Risk Level: Moderate

Mitigation: Testing will be done to ensure that the delivered product properly meets the requirements as well as ensuring that it does not break any existing functionality.

3.2.4. Use of External Systems/Products

Description: The use of cloud services like OneDrive and GitHub as well as the use of Google Docs and their API means that our group becomes reliant on their continued operation as well as needing to conform how they work.

Probability: 2 – Unlikely for cloud services to go down since they have more redundancy that we can accomplish. Other systems in use will be well documented so it will be possible to use in a manner that suits our purposed and can be documented in their use.

Impact: 2 – If a cloud service were unavailable, there is 6 group members with local copies. Third party solutions can be integrated with local storage solutions to avoid relying on an online service.

Risk Level: Low

Mitigation: Local copies of the project and documentation will be kept on local devices to ensure that work can still be done if cloud storage services go down. Once services are up again, local copies will be merged to update the online copies to be up to date once more.

4. Resource Management

4.1. Resources

4.1.1. People

Our group consists of 6 people, each with differing schedules as to when work can be done. In addition to the group, we have a project sponsor who has brought the project forward with its requirements and is acting as the client for this project.

Everyone has a role assigned to them that will dictate what aspect of the project they are working on, while these roles are what each group member is mainly working on, each member of the group is welcome to work on any part of the project.

Because of the varying schedules of everyone involved, there have been dedicated meeting times organized to ensure everyone can meet and be on the same track. These meeting times have been detailed in Section 9 as a part of the Quality Manual.

People as resources will being used for the whole project in all areas of the project with roles potentially changing and people needing to be flexible in roles throughout the project.

4.1.2. Hardware

Each member of the group has their own computer for development and testing, this will be the main piece of hardware in use for most of the project.

Our solution may utilize third party cloud instances for hosting our application or for storage. Should this be the case, an Amazon AWS or Microsoft Azure server instance will be used.

4.1.3. Software

For the solution, we will be using a starter template based on Portant's application with Google Auth and Docs API support that can authenticate users and write to Google docs the contents of a web form. Having this template as a starter allows for easier development in line with Portant's existing products and puts more emphasis on security development rather than transfer protocols.

For development, the language used is a mixture of Python for the back-end application operations and JavaScript for front-end webpage operations. Both languages will employ libraries to extend their functionality for development.

The Flask library for Python will be used to set up a web framework for the application. This will be used to create and link pages and establish the interactions between parts of the application.

MongoDB, a database creation and management library for Python will be used to enable the creation of a database to store and retrieve relevant application data for when it's required.

The JSEncrypt and RSA libraries for JavaScript and Python respectively will be used to perform cryptographic functions on data for security purposes.

Version control software will also be utilized, with GitHub being where the codebase is located and Word Online being where documentation will be located. GitHub is an industry standard version control system for code and will make it easier to keep group members up to date on where progress is being made in development. This also ensures that we have redundancy if local copies of the project are either lost or damaged. Word Online offers the same version control and redundancy but for the project documentation.

All the above-mentioned pieces of software will be used during the development phases of the project, when the application is being built from the template to include the sponsor's requested features.

Software being used for the testing and security evaluation stages of the project will include things like Wireshark, Kali Linux, TCPDump, among many other things will be used once the framework is in place to conduct security analysis and testing. This would take place during the later stages of development and after development is completed, giving the security team time to properly find the weaknesses in the system and for them to be fixed.

4.2. Organization

Project Role	Team member	Role Description	Contatct Information
Project Sponsor	Blake Lockley	Sets out the requirements and acts as the client, ensuring the project is on the right track	Email: blake@portant.co
Project Manager	Arshita Jaryal	Organizes project meetings, deadlines and ensures project is on track	Email: arshita.jaryal@students.mq.edu.au
Project Developer	Socheat Chhun	Develops the framework for the application and assists with implementation of security measures	Email: socheat.chhun@students.mq.edu.au
Project Developer	Jarrod Adair	Develops the framework for the application and assists with implementation of security measures	Email: jarrod.adair@students.mq.edu.au

Security	Md Mehedy Hasan	Designs and implements security and encryption measures for the project	Email: md-mehedy.hasan@students.mq.edu.au
Security	Edward Morris	Designs and implements security and encryption measures for the project	Email: edward.morris@students.mq.edu.au
Document Manager	Bradley Anderson	Responsible for laying out documentation, writing, editing, and formatting	Email: bradley.anderson@students.mq.edu.au

5. Project Deliverables and Schedule

5.1. Deliverables Due

Throughout this project we will be writing scoping and design documents that will lay out the scope of what the project needs to accomplish and how it will be done. The diagrams that can go along with these are wireframe diagrams for application interface designs and the screen flow, dataflow diagrams can also be used to show how data will flow between points in the application and what is done to that data security-wise.

When the project is to be handed over to the sponsor, including the documents mentioned above it will also include an application with transport and security protocols that match what the requirements of the project were. The application will also come with a user manual which will guide new users on how to navigate the UI and the workings of the application.

5.2. Process Model

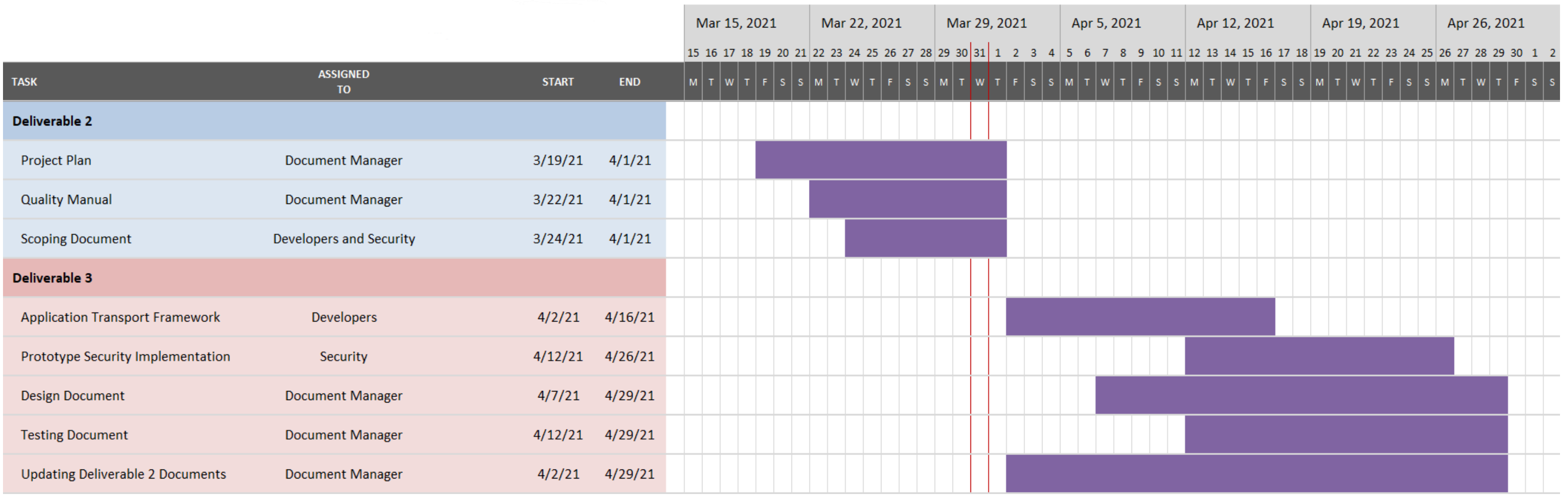
The process model in use for this project will be that of the Agile methodology. The development of an application that can query for and deliver information to a Google document in a secure format will be delivered in stages as the weeks go on.

Agile will allow for progress to be made on the project over the course of a week before being able to show the progress made to the project sponsor. From this, feedback as to what can be implemented next/changed to fit the requirements that the sponsor has set out. A project can be built up over the course of the timeframe we have and with demonstrations at intervals throughout the semester there are deadlines that must be met with where the project needs to be at that point.

Since there will be regular meetings, requirements can be adjusted based on progress made with the project at that point. Requirements can be added onto or scaled back to ensure that the project is constantly evolving if good progress is being made or reined in to ensure that a minimum viable product is achieved if progress is being halted for one reason or another.

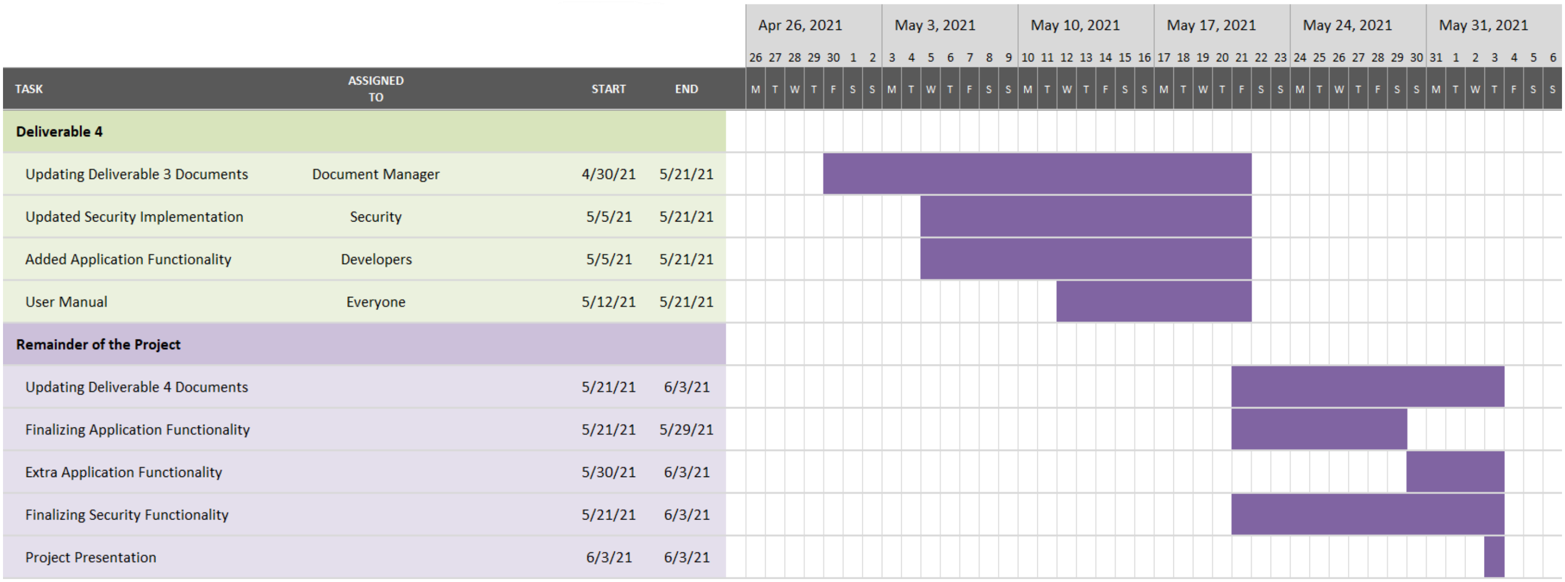
5.3. Gantt Chart

The Gantt Chart for the project. The project is listed as being started from the 19th of March (When work on Deliverable 2 started) and assumes the end of the project is the 3rd of June (When the presentation happens) as the finalized product would be handed to the sponsor not long after the presentation.



TASK	ASSIGNED TO	START	END
Deliverable 2			
Project Plan	Document Manager	3/19/21	4/1/21
Quality Manual	Document Manager	3/22/21	4/1/21
Scoping Document	Developers and Security	3/24/21	4/1/21
Deliverable 3			
Application Transport Framework	Developers	4/2/21	4/16/21
Prototype Security Implementation	Security	4/12/21	4/26/21
Design Document	Document Manager	4/7/21	4/29/21
Testing Document	Document Manager	4/12/21	4/29/21
Updating Deliverable 2 Documents	Document Manager	4/2/21	4/29/21

Figure 1: The Gantt Chart for Deliverables 2 and 3 for the project



TASK	ASSIGNED TO	START	END
Deliverable 4			
Updating Deliverable 3 Documents	Document Manager	4/30/21	5/21/21
Updated Security Implementation	Security	5/5/21	5/21/21
Added Application Functionality	Developers	5/5/21	5/21/21
User Manual	Everyone	5/12/21	5/21/21
Remainder of the Project			
Updating Deliverable 4 Documents		5/21/21	6/3/21
Finalizing Application Functionality		5/21/21	5/29/21
Extra Application Functionality		5/30/21	6/3/21
Finalizing Security Functionality		5/21/21	6/3/21
Project Presentation		6/3/21	6/3/21

Figure 2: The Gantt Chart for Deliverables 4 and the conclusion of the project

6. Handover Requirements

The sponsor of the project has specified that they want 2 things handed over to them by the end of the project, these being:

1. The source code of the application being developed. This will include the files containing the code, environment files and README files that are required to set up the environment the application runs on.
2. Supporting documentation that consists of the documents that have been completed throughout the project. This consists of the Feasibility report, Project Plan, Quality Manual, Scoping Document and Design Document. These documents will encompass things like the development schedule and technical documentation on the application’s workings and security functionality.

These things will allow the sponsor to see the progress that has been made towards creating the proof-of-concept that they had originally wanted and will enable them to continue the development/use of the developed application as they see fit.

7. Quality Control and Management

7.1. Project Deliverables Reports

Quality standards – Client standards.

Acceptance criteria – Approval from client.

Quality assurance activity – Regular communication with the sponsor to ensure that documentation reflects the desired requirements and outcomes of the project.

Timeframe – Throughout the project (~10 weeks).

People responsible – All team members.

7.2. Document Management

Quality standards – Client standards & Document criteria

Acceptance criteria – Review by document manager and

Quality assurance activity – Editing, formatting, and proofreading to ensure documentation is legible and is easy to understand.

Timeframe – Entire Project (~10 weeks).

People responsible – Bradley Anderson.

7.3. Compliance with standards

Quality standards – GDPR (General Data Protection Regulation), OAIC (Office of the Australian Information Commissioner), NIST (National Institute of Standards and Technology), CSF (Cybersecurity Framework).

Acceptance criteria – That the application follows the data protection protocols set out in each of these regulations and standards.

Quality Assurance activity – Use of industry standard security and encryption techniques for the storage and use of data.

Timeframe – Entire Project (~10 weeks).

People responsible – Project Developers and Security.

7.4. Application development

Quality standards – The OECD.

Acceptance criteria – The application falls within the guidelines and standards set out by the OECD.

Quality Assurance activity – We read and follow the development standard that is set out in the OECD quality development manual.

Timeframe - Week 4 – Week 12 (Planned)

People responsible – Jarrod Adair, Socheat Chhun.

7.5. Security Implementation

Quality standards – Client requirements

Acceptance criteria – The security measures put in place are given approval by the client sponsor and meet basic security standards.

Quality Assurance activity – Product demonstrations to the sponsor with supporting documentation as to security measures in place.

Timeframe – Deliverable 2 to end of the project (29th April – Late June)

People responsible – Md Mehedy Hasan, Eddie Morris.

7.6. Contribution to the project

Quality standards – Team standards and marking criteria.

Acceptance criteria – All team members contribute meaningful work to the project in roughly equal amounts and that said work contributes towards fulfilling the project deliverables.

Quality Assurance activity – Team performance evaluation form and Deliverables certificate.

Timeframe – Entire Project

People responsible – All team members

7.7. Communication protocol

Quality standard – Easy to communicate with and convenient to meet for all members.

Acceptance criteria – Team approval of meeting formats and times.

Quality assurance activity – Team discussion.

Timeframe – Whole project.

Person responsible – All team members.

8. Reviews, Audits and Testing

Quality control Item	Reviews, Audits and Testing
Project Reports	Review each week by sponsors and all team members and update accordingly.
Document management	Documents are constantly being checked by document manager to fix errors, mistakes and format the documents to be in a neater format.
Compliance and standards	Review against industry standards and compliance documents and maintain the compliance and standards.
Application development	Reviews of the project will be done by both the sponsor and team members to ensure they are compliant with requirements. Tests to ensure all implemented features are functional and working as intended will be done by developers and detailed in the testing document.
Security implementation	Implement security mechanism and collaborate with developer and presentation of information to the clients in regular meetings and get feedback from client. Reviews of security measures implemented will be done by the security team and the sponsor. Tests and audits of security effectiveness and strength will be conducted by the security team and recorded in the testing document.
Contribution to the project	Conduct individual performance review based on contribution to documentation and project repository. Team discussions and evaluations will be done in deliverables certificate and contribution forms.
Communication protocol	Review of communication channels and the ways things are being communicated will be done to ensure that communication channels are being used effectively and the way information is being communicated is suitable.

9. Tracking and Change Management

To perform change management and tracking, we will be using GitHub and Word Online for the project. GitHub is a version control system for code bases which allows for projects to be backed-up, shared and added to online repositories. One good feature of this software is that changes can be stored on separate branches for experimentation with different implementations without breaking the existing codebase. If something does break, we are able to roll back the changes to the last working version and continue from there. We can use this software to do a comparison of implementations to see which one is the better one should there be two or more ways to implement certain features of our application.

Documentation will be kept on Word Online, which much like Google Docs allows multiple people to be working on one document at once. Changes made to the document will be logged and can be rolled back to if several changes made need to be removed. Much like GitHub, Word Online allows for backups, collaborative working and rollbacks and as such will be used for change management and tracking for the documentation for the project.

Both platforms allow for people's contributions to be attributed to them so it will make it easier to see who has worked on what parts of the project and will allow us to accurately assess contribution by each member of the group.

10. Communication

Communication type	**Objective of communication**	**Medium**	**Frequency**	**Audience**	**Deliverable**
Kick-off meeting	Introduce the project team and the project. Review project objectives and management approach.	Zoom	Once-off	Project sponsor, Project team members	None
Weekly meeting with sponsor	Report, discuss, review and general Q&A	Zoom	Weekly (On Tuesdays)	All team members and project sponsor	All deliverables
Weekly Team meeting	Getting all group members up to date	Zoom	Weekly (On Sundays)	All team members	All deliverables
Email communication	Clarify things outside of meeting times and ensure work is on track	Email	As many times as needed	Project sponsor, any team member/s	All project matters (documents or development)

11. Conflict Resolution

There may be points in the project where conflict arises either between team members and the sponsor over things like requirements or implementation. Alternatively, there could be conflicts between team members over workload, roles, and responsibilities.

As a first point of call, the team should aim to talk things over with each other. If it is a dispute with the sponsor the whole team should try to weigh in and come to a resolution. If the dispute is between team members, then the sponsor can be brought in as an unbiased 3rd party to offer suggestions to resolve the dispute. One way to resolve things in both cases would be to write down both side's points and aim to find a middle ground that satisfies both parties without going to extremes.

If neither of these options work, the issue can then be escalated to the unit co-ordinators for a solution to the issue. They can either talk to the parties involved and aim to straighten things out or should the problem be unnegotiable reorganize groups or sponsors to get the project back on track and completed to the best of the group's ability.

12. Appendix

Standards and frameworks

NIST Cyber security framework version 1.1

Compliance

OAIC - Office of the Australian Information Commissioner

GDPR - General Data Protection Regulation

Team performance evaluation form	
Team name____________	Date___________
Personal evaluation	
5=excellent, 4=Good, 3=Acceptable, 2=Marginal 1= Unacceptable	

Team member name						
Attended team meetings.						
Was punctual.						
Was willing to listen others.						
Helped to identify and clarify problems.						
Was willing to discuss disagreement and adapt.						
Helped everyone to understand solution.						
Contributed equally.						
Communicated regularly.						
Taken initiative.						
Member total contribution						

Results:
Over 75% = Good or Excellent
60% - 74% = Above average
45% - 59% = Average
Less than 45% = Bad or Too little