*[Cyber Incident Response Plan Objectives and Evaluation]*

**Project Plan**

*[CIRPAE R&D]*

*List of your Names*:

| **Name** | **Position** | **email** | **phone** |
| --- | --- | --- | --- |
| **Aidhan Mitsopoulos** |  | 103598809@student.swin.edu.au | 0428770628 |
| **Habib MUSTAFAWI** |  | 102053200@student.swin.edu.au | 0466368916 |
| **Numil Fernando** |  | 103517163@student.swin.edu.au | 0406164700 |
| **Thomas Davis** |  | 103203475@student.swin.edu.au | 0449619570 |
| **Huy Tran** |  | 102559614@student.swin.edu.au | 0403204649 |
| **Zahin Un Nafi** |  | 103539510@student.swin.edu.au | 0481834630 |

*SUBJECT CODE, NAME, SEMESTER AND DATE*

|  |  |
| --- | --- |
|  | | **Note: Please read carefully**  Throughout this document, all text in ***RED ITALICS*** should be replaced with data relevant to your project.  Delete all the explanatory text in RED, including this box before submission. | | --- | |

# 

# **Document Change Control**

| **Version** | **Date** | **Authors** | **Summary of Changes** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*[Each time this document is revised, complete details of changes in Document Change Control table]*

# **Document Sign Off**

| **Name** | **Position** | **Signature** | **Date** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*[When document is finalised for submission, all team members must affix their signature in the Document Sign Off table]*

***[No-one should sign unless they have read the report and agree with it. ]***

# **Client Sign off**

| **Name** | **Position** | **Signature** | **Date** |
| --- | --- | --- | --- |
|  |  |  |  |
| **Organisation** | | | |
|  | | | |

*[Client to sign off on the Project Plan to signify they agree with the plan]*

# **Contents**

Introduction

1.1. Background

1.2. Key Project Personnel

1.2.1. Client

1.2.2. Other Stake holders

1.2.3. Project Supervisor, Team Leader and Key Project Members

2. Terms of Reference

2.1. Objectives

2.2. Scope

2.3. Critical Success Factors

2.4. Acceptance Criteria

3. Establishment

3.1. Processes, Procedures and Standards

3.2. Project Environment

3.3. Project Team Skill Development Requirements

4. Deliverables, Activities and Capital Resources

4.1. Deliverables

4.2. Activities

4.3. Resources

5. Organisation and Structure

6. Risks

7. Schedule

7.1. Project Time Line

7.2. External Dependencies

7.3. Assumptions

8. Budget

9. References

10. Tables Index

# 

# 

# **Introduction**

*[Briefly explain what the purpose of this document is, who should read it and how it will assist with the project development]*

The goal of this project is to create a Cyber Incident Response Plan and Evaluation system (CIRPAE) for Retrospect Labs. This document is meant for the project team, client, and other project stakeholders.

The project plan outlines the various activities that will be carried out in order to achieve the project objectives, such as collecting and analysing incident response plans, training a machine learning model with natural language processing techniques, and creating incident dialogue for validation purposes. It also provides details on the project scope, critical success factors, acceptance criteria, processes, procedures and standards, project team, risks, schedule, budget, and references.

By adhering to this project plan, the project team will be able to develop a complete CIRPOE system for Retrospect Labs in a timely and cost-effective manner. The plan will serve as a project roadmap, including essential activities and deliverables, as well as deadlines and resources needed. The plan will also help the client understand the project's scope, goals, and risks, and it will serve as a foundation for continuous project management and assessment.

# **1.1.** **Background**

*[Describe how this project (****not the software****) came into being and who the main players are.*

*Discuss the overall driving forces behind the project and provide some insight into the organisations involved and the nature of the business domain]*

The Cyber Incident Response Plan and Evaluation (CIRPAE) project was initiated by Retrospect Labs to develop a comprehensive and effective incident response plan to cyber threats. The main goal of the project is to create an incident response strategy that Retrospect Labs and its clients can utilise to react to cyber threats swiftly and efficiently, safeguard vital assets, and limit the impact of events on company operations.

The rising frequency and severity of cyber attacks is driving the initiative. Cyber assaults have grown in sophistication, frequency, and severity, presenting a serious risk to enterprises of all kinds. This has made it critical for companies to be prepared to react to events promptly and efficiently. Retrospect Labs has undertaken this project to establish a thorough incident response strategy in response. The nature of the business domain necessitates a comprehensive and well-defined incident response strategy that addresses many sorts of cyber events, such as ransomware, phishing, and other types of cyber-attacks.

The project team, client, and other stakeholders are all key players in the CIRPAE project. The project team, which comprises a project supervisor, team leader, and key project members, is in charge of developing and implementing the CIRPAE system. Retrospect Labs, the project's client and sponsor is actively involved in project planning and implementation.

# **1.2.** **Key Project Personnel**

The key personnel involved in this project are as follows:

* **Client:** Retrospect Labs
* **Project Supervisor:** Dr. Naveed Ali
* **Team Leader:** Aidhan Mitsopoulos
* **Key Project Members:**

1. Habib Mustawafi
2. Huy Tran
3. Numil Fernando
4. Thomas Davis
5. Zahin Un Nafi

# 

# **1.2.1.** **Client**

*[Discuss briefly your client]*

Retrospect Labs is a cybersecurity company founded in 2019 by former Australian Government Incident Responders, Jason Pang and Ryan Janosevic. CyRise, a venture-backed accelerator programme, accepted the startup in 2020. The objective of Retrospect Labs is to make cybersecurity accessible to all organisations by delivering creative, dependable, and cost-effective security solutions.

Retrospect Labs specialises in offering a platform for businesses to mimic different cyber threat situations, allowing them to educate their employees in proper cyber incident response. Companies may use Retrospect Labs' platform to run cybersecurity exercises and drills that simulate real-world scenarios and evaluate their capacity to react to a broad spectrum of cyber disasters. This enables businesses to uncover flaws in their cybersecurity measures and increase their overall preparation for cyber assaults.

# **1.2.2.** **Other Stake holders**

*[Other than the client, detail the list of people who hold a stake in the project.*

*Include a description for the position and relevant contact details for each person.*

*If unknown, define roles and make suggestions about who would be suitable]*

*[A stakeholder is a person people for whom the success or failure of the project will make a difference]*

**Project Supervisor:**

The project supervisor is responsible for overseeing the project and ensuring that it is delivered on time, within budget, and to the satisfaction of the client. They will provide guidance and direction to the team leader and key project members, and will be monitoring progress while ensuring that all work is completed to a high standard.

**Contact:** Dr. Naveed Ali, email: nali1@swin.edu.au

**Team Leader:**

The team leader is responsible for managing the day-to-day activities of the project team and working closely with the team for developing the project. They will collaborate with the project supervisor and key project members to ensure that the project is delivered on time and within budget.

**Contact:** Aidhan Mitsopoulos, email: 103598809@student.swin.edu.au

**Key Project Members:**

The key project members are the individuals who will be responsible for developing the software along with the team leader and ensuring that it meets the requirements of the client.

**Contact:**

Habib Mustawafi, email: 102053200@student.swin.edu.au

Huy Tran, email: 102559614@student.swin.edu.au

Numil Fernando, email: 103517163@student.swin.edu.au

Thomas Davis, email: 103203475@student.swin.edu.au

Zahin Un Nafi, email: 103539510@student.swin.edu.au

**End-Users:**

The end-users of the software are a key stakeholder group, as the success of the project will depend on whether or not they find the software useful and easy to use. Their feedback and input will be important throughout the development process, and the team will work to incorporate their needs and preferences into the final product.

**Regulatory Bodies:**

Regulatory bodies that oversee the industry may have specific requirements that need to be met in order for the software to be used in the market. The team will need to ensure that the software meets all regulatory requirements and obtains any necessary certifications before it can be released.

# 

# **1.2.3.** **Project Supervisor, Team Leader and Key Project Members**

*[This is where you list your team, and indicate each one’s role in the project]*

| **Position** | **Name** | **Responsibilities** |
| --- | --- | --- |
| Project Supervisor | Dr. Naveed Ali |  |
| Team Leader | Aidhan Mitsopoulos |  |
| Key Project Member | Habib Mustawafi |  |
| Key Project Member | Huy Tran |  |
| Key Project Member | Numil Fernando |  |
| Key Project Member | Thomas Davis |  |
| Key Project Member | Zahin Un Nafi |  |

# **2.** **Terms of Reference**

*[State the goal the project (not the software). What the client envisioned it to achieve and who are the intended user group. This may not be measurable or tangible]*

# **2.1.** **Objectives**

Objectives

* The GPT model is able to receive a CIRP and determine the objective
* The GPT model is to be able to comprehend security threats
* The GPT model is able to analyse a piece of dialogue and determine if the objective has been met by standards of a CIRP.
* Determine validity of CIRP by comparing it against alternative CIRP’s

Objectives:

* The GPT model is able to analyse a piece of dialogue and determine if the objective has been met by standards of a CIRP.
* Determine validity of CIRP by comparing it against alternative CIRP’s based off our human knowledge.
* Model is capable of reading through a scenario and identifying possible threats within said instance.
* The GPT model is to be able to comprehend security threats.
* GPT Model should follow the criteria of C.I.A (Confidentiality, Integrity, Accessibility.)
* Develop a user friendly interface so non experienced users can access it’s functions.

*[Identify the objectives (about 3 to 10) of the project that are at a high level breakdown of the goal. These objectives must* ***be measurarble*** *and listed in the order of* ***importance****. The success of the project is determined by how well the objectives are met]*

*[The client must* ***approve*** *the list of objectives]*

# **2.2.** **Scope**

We have decided to train a ChatGPT model to be able to be fed sums of Cyber Incident Response Plans and Evaluate the Objectives from each document. The AI will not be able to provide steps on how to mitigate an attack or a potential threat, it will only be able to identify the objectives from each CIRP. The AI is also not expected to form a CIRP from the objectives it receives from it’s consumed CIRP’s. The AI will be fed data through the use of the Python Library known as Beautiful Soup from any HTML or XML file that contains a cyber incident response plan and output dotpoints of paragraphs or sentences that surmise the objectives it identified from each CIRP.

*[Define the boundaries of the project. Specify what the project will and will not accomplish and the earliest start and latest finish dates]*

***\*\*\* This is very important \*\*\****

# **2.3.** **Critical Success Factors**

* The AI is to be able to surmise the Objectives pulled from each CIRP in clear concise sentences.
* The Objectives the AI identified have to match the Objectives we humans Identify and automate it through a much larger scale.
* The AI must follow the format of the Cyber Security Triad known as C.I.A to properly follow industry standards.
* The AI is to be able to read through a scenario and identify the flaws each objective of the scenario based off it’s knowledge.

*[Identify the factors (about 3 to 6) which have the most influence on the success of the project. These should be* ***based on your objectives, but they are NOT THE SAME****]*

*[They are ways of measuring if you’ve met the objective. For example, usability requirements,* ***metrics*** *and specifications]*

*[Identify those factors which if absent will cause the project to fail]*

# **2.4.** **Acceptance Criteria**

* The numerous of CIRP’s fed into ChatGPT must have a high percentage of Objectives that properly follow Cyber Security Objectives e.g C.I.A
* User Guide is to be provided so that he is capable of manipulating the trained software properly.

*[Briefly describe what will be considered acceptable by the client, and explain how the client will determine if the software is acceptable]*

*[Refer to the Scope and Critical Success Factors above, and look up how to conduct acceptance testing]*

# **3.** **Establishment**

# **3.1.** **Processes, Procedures and Standards**

*[This section should refer to the methodology used.*

- *Identity a software development method that will be adopted for the project and discuss why it was chosen by the team for the project.*

- *Identify processes that will be adopted in the project, such as*

o *Versioning system*

o *User-Centred Design Process*

- *Identify and discuss briefly the program coding standards that will be adopted for this project]*

# **3.2.** **Project Environment**

*[Identify work places, computers, user accounts, server accounts, DBMS, and stationary required for software development, and later for software deployment]*

# **3.3.** **Project Team Skill Development Requirements**

*[Identify any training necessary for members of the project team]*

# **4.** **Deliverables, Activities and Capital Resources**

# **4.1.** **Deliverables**

*[List and describe specific deliverables that will be completed. deliverables are things you give to the client or the project supervisor]*

*[For example, software, manuals, documentation, poster, video, test results]*

# **4.2.** **Activities**

*[List and describe specific activities that will be executed in order to produce the deliverables as listed in section 4.1. For example, you can use phases, stages and activities defined in the selected process or lifecycle]*

*[In describing the activity, identify, list, and describe the task(s) involved in each activity. Each activity is made up of one or more tasks]*

# **4.3.** **Resources**

*[List and describe specific resources needed in order to complete the project]*

*[Resources are things you need to do the project which may be provided by your client or university. For example, equipment, room, software library]*

# **5.** **Organisation and Structure**

*[List all the groups of people that will be involve or has a role in the project, Be sure to include every role (especially business users who will be interviewed during the requirements modelling and those involved in acceptance testing]*

*[This is not just your team. It is anyone else who has direct interaction with the project. This also includes people will be interacting with the software – e.g. people who test it or are interviewed about it, and other members of their organisation)]*

*[Describe the organisational structure that will be used during the project. For example, a matrix structure may be used in describing role of each group. This enables the person responsible for the activity or deliverable to see the groups of people to me managed]*

| ***Activities***    ***Deliverables*** | ***From 4.2*** |  |  |  |
| --- | --- | --- | --- | --- |
| ***From 4.1*** | *Group involved* | *as identified* | *above* |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 1 Activities and Deliverables

# **6.** **Risks**

*[Discuss any major risks that could affect your project plan]*

*[This is not a full risk analysis but more of a look at the risks that affect the running of the project]*

*[Take this seriously. When things start to go wrong, you will be expected to follow the strategies outlined here. Explain mitigation strategies in detail. Number each strategy and place the number in the table above]*

*[For each Risk record the following*

• *Rank*

• *Name*

• *Description*

• *Likelihood of occurrence*

• *Severity*

• *Strategy for mitigation (prevention)*

• *Contingency or fall-back position should the risk manifest itself. (plan B)- not an elaboration of the mitigation strategy]*

•

**Risks associated with this project.**

| **Rank** | **Name /**  **Description** | **Occurrence**  **Probability**  **(H/M/L)** | **Severity**  **(H/M/L)** | **Mitigation**  **Strategy**  **Number** | **Contingency** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 2 Risks

# **7.** **Schedule**

# **7.1.** **Project Time Line**

*[Given the tasks (group as activities) in Section 4.2, schedule each tasks using a Gantt chart or some other type of time line. You do not have to use Microsoft Project. Acceptable Gantt charts can be created using Excel or various graphics programs or can be hand-drawn]*

*[For each task, show the deadline, and who is allocated to each task (your team members). Often it is better to allocate two people to each task in case one becomes unavailable (e.g. breaks a leg)]*

# **7.2.** **External Dependencies**

*[Describe any inputs from external parties that are required to ensure that the schedule is met. These dependencies, if any, must also be indicated in the time line (Section 7.1) as a critical point]*

# **7.3.** **Assumptions**

*[Describe any assumptions that have been made in arriving at the schedule. These may be critical to the implementation of the software]*

# **8.** **Budget**

*[Summarise in a table the rate per hour for each of the team member. Look for an appropriate rate per work when doing such type of project. Using the role listed in Section 1.2.3, complete the table below]*

**Personnel Cost**

| **Name** | **Rate per Hour** |
| --- | --- |
|  |  |
|  |  |
|  |  |

Table 3 Personnel Cost

*[List all the tasks (grouped as activities) described in Section 4.2 in a table and estimate the number of hours needed to complete each task]*

**Time Estimated to Complete Each Task**

| **Activity** | **Task** | **Estimated hours needed (hrs)** | **Total per activity (hrs)** |
| --- | --- | --- | --- |
| ***1*** | *A* | *10* |  |
|  | *B* | *15* |  |
|  | *C* | *20* |  |
|  | *D* | *5* | *50* |
|  |  |  |  |
|  | *F* | *5* | *10* |
|  |  | Total |  |
|  |  |  |  |

Table 4 Task time estimate

*[As a guide in estimating the time consider the following:]*

*[Each team member should contribute equally, and time spent actually writing software should be about (200 hours x number of team members, ie, about 10 hours per week per member, excluding lectures) across the 2 semesters,*

*Total time allocation for each student should not exceed 10 hours per week,*

*The total hours per activity should be feasible within the schedule defined in Section 7.1]*

*[Note that the schedule in Section 7.1 includes slack time]*

# **9.** **References**

*[If you have used information from published sources, show where it came from. Use the Harvard system of citation. For instance, if it is from a website]*

***Your reference list entry must be in the form of***

**Author, Initial(s) Year, *Title of Document/Webpage/Website*, Organisation/Host, viewed Day Month Year, <URL>.**

example

Yates, J 2009, *Tax expenditures and housing*, Australian Housing and Urban Research Institute, viewed 12 November 2013, <http://www.ahuri.edu.au/publications/download/ahuri\_judith\_yates\_research\_paper>.

***Your in-text may be in the form of***

- **Direct quote**

"Most official estimates ..." (Yates 2009).

- **Paraphrase**

Yates (2009) looked at the equity implications of tax ...

***For more information on the Harvard style guide, refer to***

<http://www.swinburne.edu.au/lib/studyhelp/harvard_style.html>

# **10.Tables Index**

Table 1 Activities and Deliverables. 7

Table 2 Risks. 8

Table 3 Personnel Cost. 10

Table 4 Task time estimate. 10