Student Names and Student Numbers:
Luvuyo Mcaba - ST10453348
Lebogang Maboya - ST10452993
Rio Gobi - ST10452096
Itumeleng Matjila - ST10455355
Junior Mashudu - ST10453352

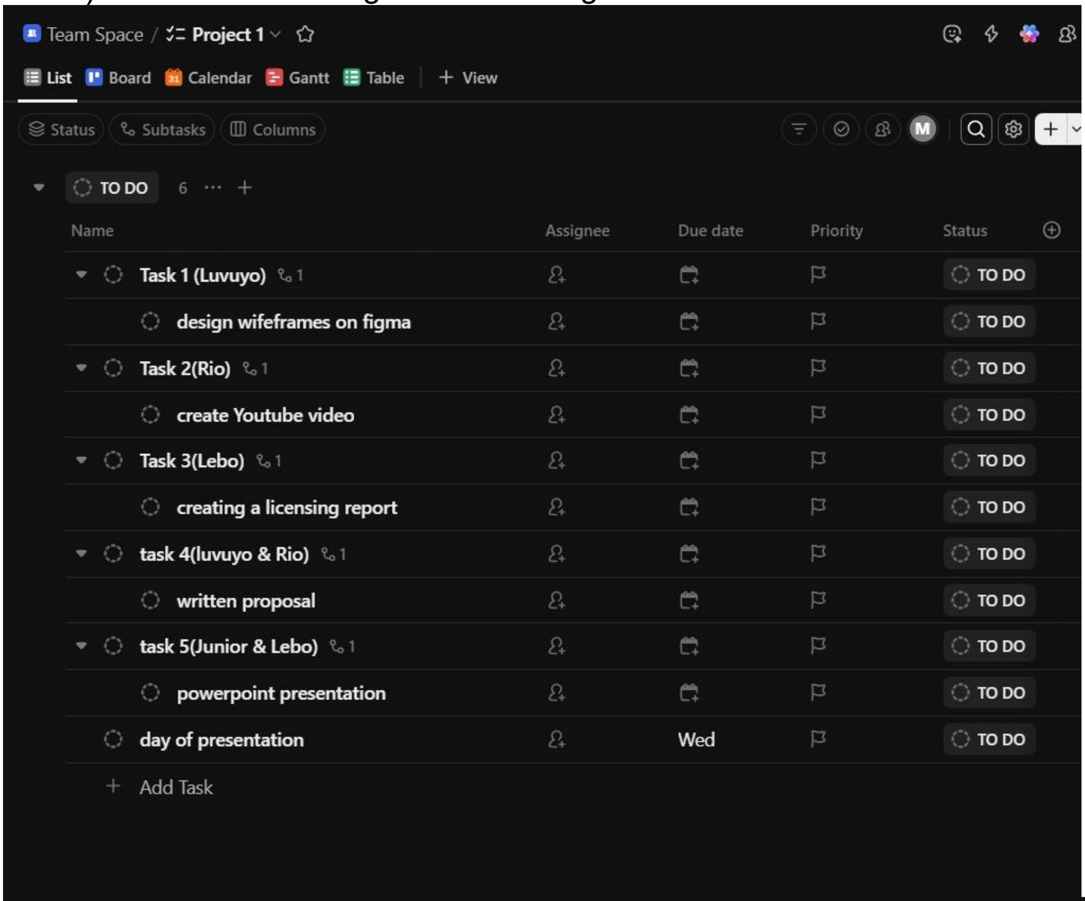
PATHWAY: ITTP5112
Lecturer: Mr. Dasram Sundesh
Date: 15 October 2025

The CuppaTime Group Work Assignment.
Assignment 2

Contents

Question 1

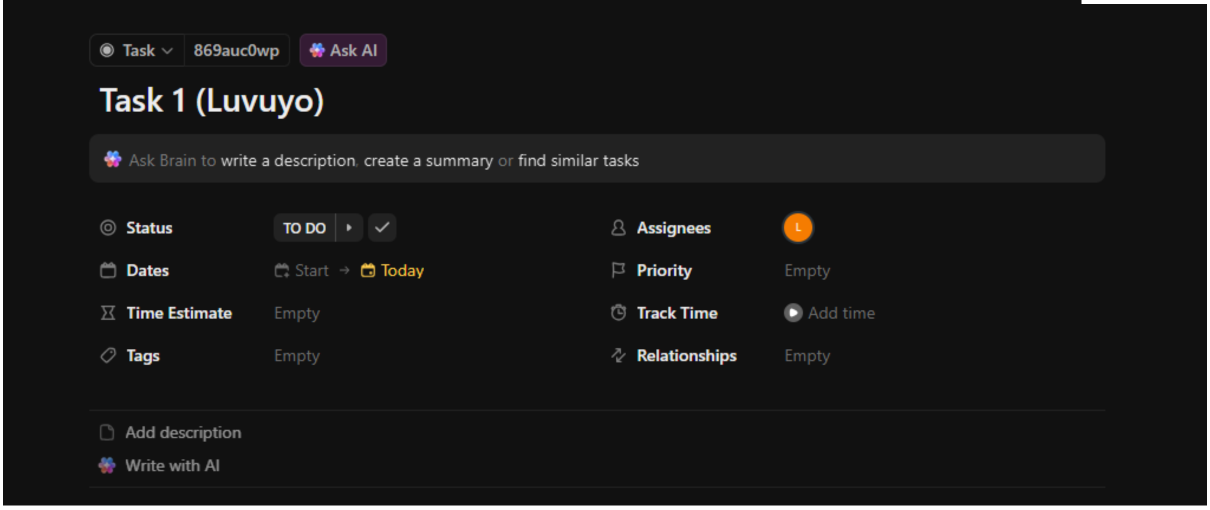
Q1.1) Screenshots of original tasks assigned:



TO DO 6 ··· +

Name	Assignee	Due date	Priority	Status
Task 1 (Luvuyo) 1				TO DO
design wifeframes on figma				TO DO
Task 2(Rio) 1				TO DO
create Youtube video				TO DO
Task 3(Lebo) 1				TO DO
creating a licensing report				TO DO
task 4(luvuyo & Rio) 1				TO DO
written proposal				TO DO
task 5(Junior & Lebo) 1				TO DO
powerpoint presentation				TO DO
day of presentation		Wed		TO DO

+ Add Task



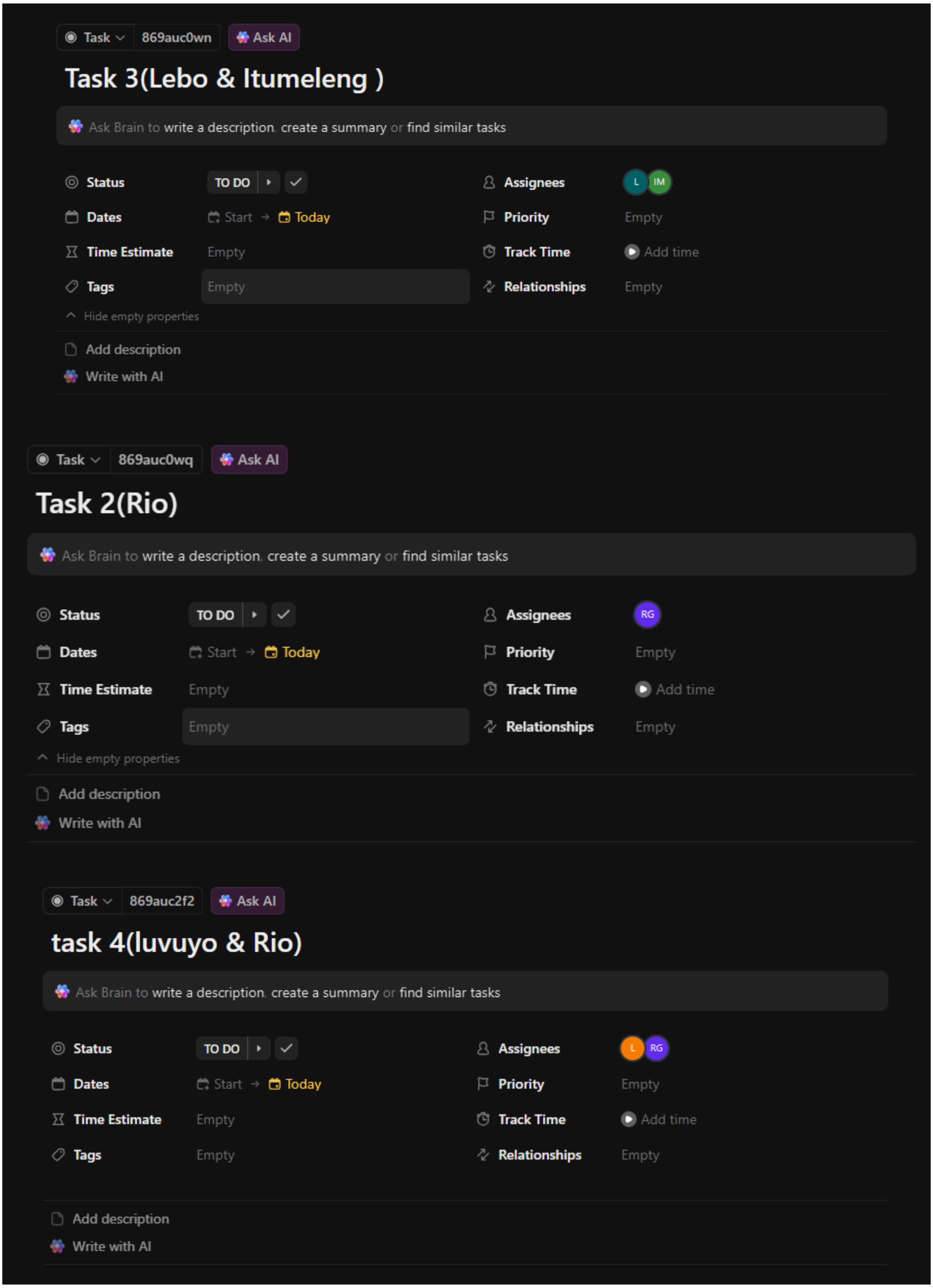
Task 1 (Luvuyo)

Ask Brain to write a description, create a summary or find similar tasks

Status	TO DO ✓	Assignees	L
Dates	Start → Today	Priority	Empty
Time Estimate	Empty	Track Time	Add time
Tags	Empty	Relationships	Empty

Add description

Write with AI



Task 869auc0wn Ask AI

Task 3(Lebo & Itumeleng)

Ask Brain to write a description, create a summary or find similar tasks

Status	TO DO ✓	Assignees	L IM
Dates	Start → Today	Priority	Empty
Time Estimate	Empty	Track Time	Add time
Tags	Empty	Relationships	Empty

Hide empty properties

Add description

Write with AI

Task 869auc0wq Ask AI

Task 2(Rio)

Ask Brain to write a description, create a summary or find similar tasks

Status	TO DO ✓	Assignees	RG
Dates	Start → Today	Priority	Empty
Time Estimate	Empty	Track Time	Add time
Tags	Empty	Relationships	Empty

Hide empty properties

Add description

Write with AI

Task 869auc2f2 Ask AI

task 4(luvuyo & Rio)

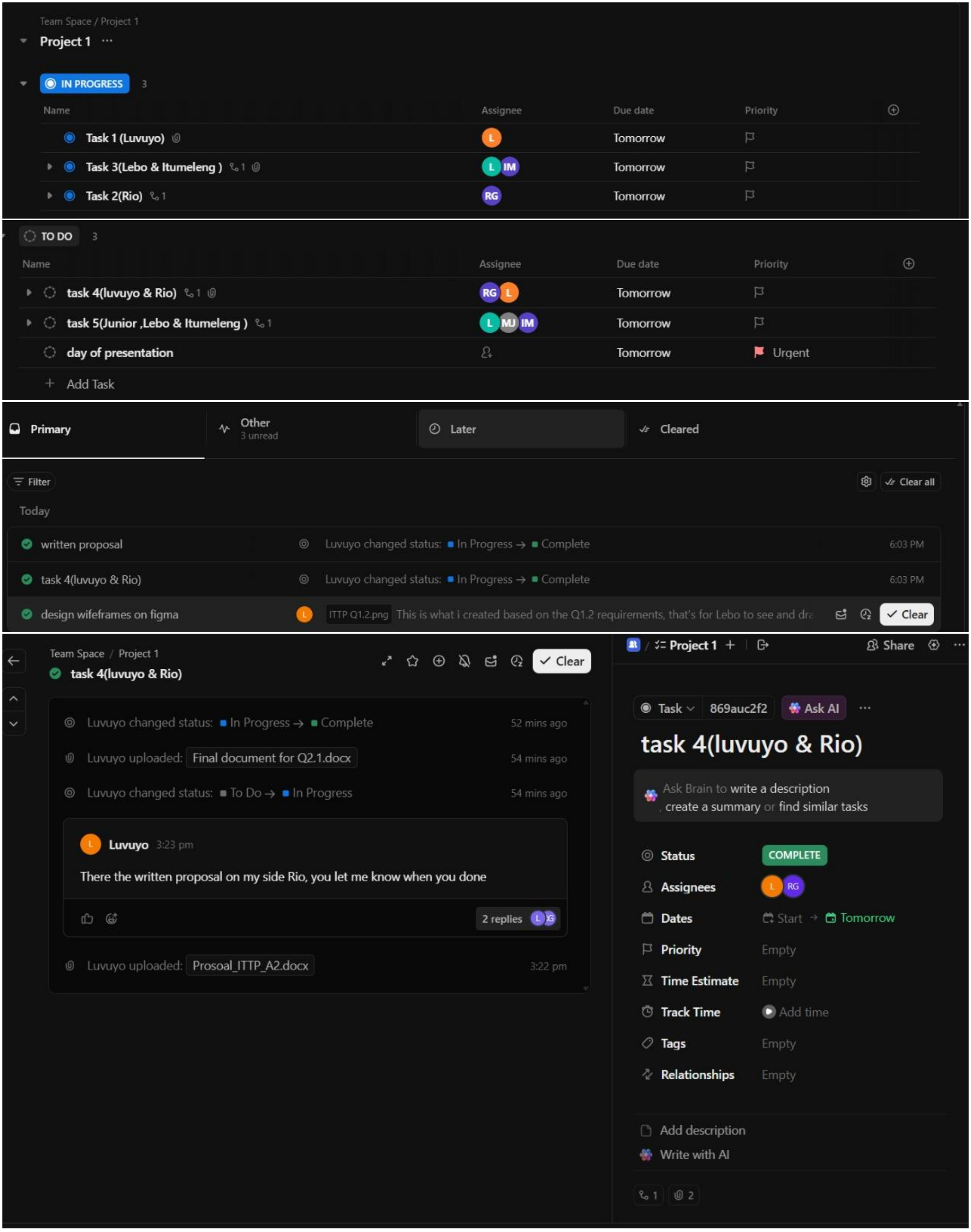
Ask Brain to write a description, create a summary or find similar tasks

Status	TO DO ✓	Assignees	L RG
Dates	Start → Today	Priority	Empty
Time Estimate	Empty	Track Time	Add time
Tags	Empty	Relationships	Empty

Add description

Write with AI

Screenshots of status updates and the completion of tasks:



Team Space / Project 1

Project 1

IN PROGRESS 3

Name	Assignee	Due date	Priority
Task 1 (Luvuyo)	L	Tomorrow	
Task 3(Lebo & Itumeleng) 1	L IM	Tomorrow	
Task 2(Rio) 1	RG	Tomorrow	

TO DO 3

Name	Assignee	Due date	Priority
task 4(luvuyo & Rio) 1	RG L	Tomorrow	
task 5(Junior ,Lebo & Itumeleng) 1	L MJ IM	Tomorrow	
day of presentation		Tomorrow	Urgent

Add Task

Today

written proposal		Luvuyo changed status: In Progress → Complete	6:03 PM
task 4(luvuyo & Rio)		Luvuyo changed status: In Progress → Complete	6:03 PM
design wifeframes on figma	L	ITTP Q1.2.png This is what i created based on the Q1.2 requirements, that's for Lebo to see and dra	

Team Space / Project 1

task 4(luvuyo & Rio)

Luvuyo changed status: In Progress → Complete 52 mins ago

Luvuyo uploaded: Final document for Q2.1.docx 54 mins ago

Luvuyo changed status: To Do → In Progress 54 mins ago

Luvuyo 3:23 pm

There the written proposal on my side Rio, you let me know when you done

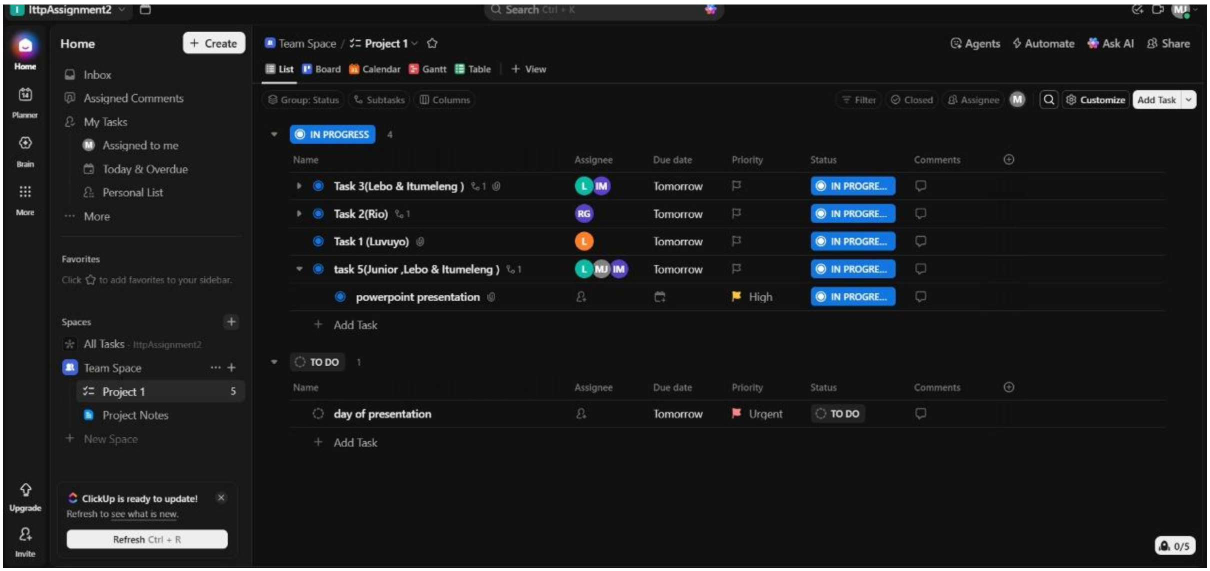
2 replies

Luvuyo uploaded: Prosoal_ITTP_A2.docx 3:22 pm

task 4(luvuyo & Rio)

Ask Brain to write a description , create a summary or find similar tasks

Status	COMPLETE
Assignees	L RG
Dates	Start → Tomorrow
Priority	Empty
Time Estimate	Empty
Track Time	Add time
Tags	Empty
Relationships	Empty



IN PROGRESS 4

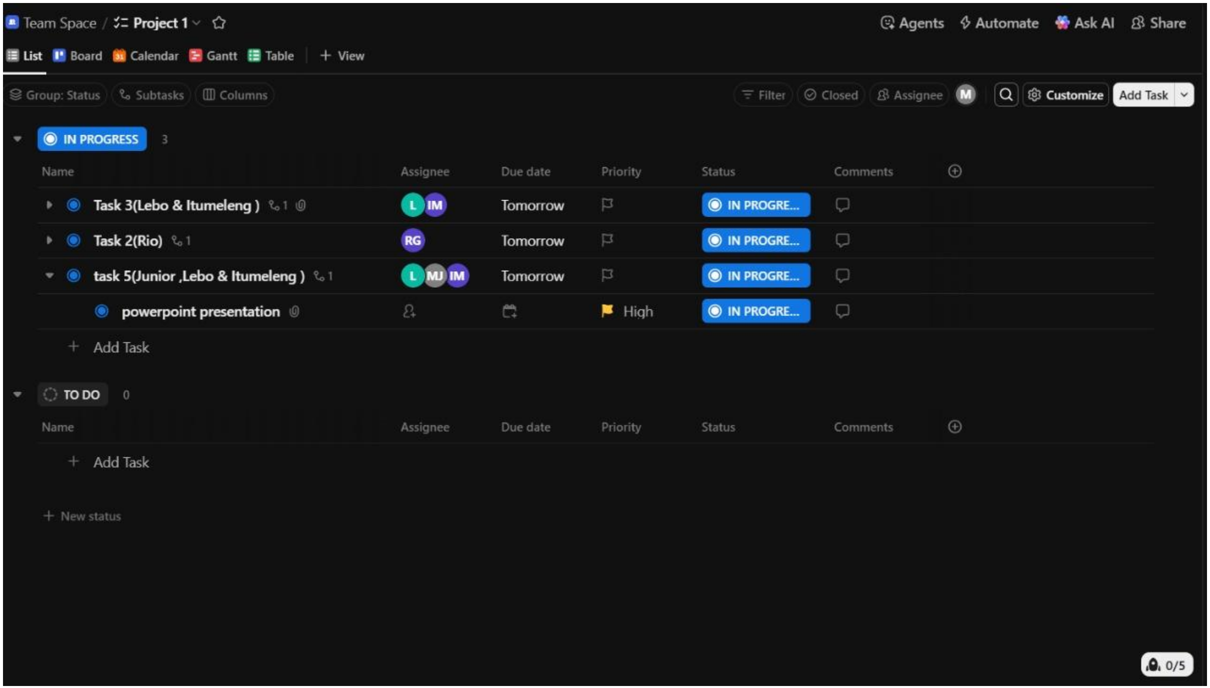
Name	Assignee	Due date	Priority	Status	Comments
Task 3(Lebo & Itumeleng) 1	L IM	Tomorrow		IN PROGRE...	
Task 2(Rio) 1	RG	Tomorrow		IN PROGRE...	
Task 1 (Luvuyo)	L	Tomorrow		IN PROGRE...	
task 5(Junior ,Lebo & Itumeleng) 1	L MJ IM	Tomorrow		IN PROGRE...	
powerpoint presentation			High	IN PROGRE...	

+ Add Task

TO DO 1

Name	Assignee	Due date	Priority	Status	Comments
day of presentation		Tomorrow	Urgent	TO DO	

+ Add Task



IN PROGRESS 3

Name	Assignee	Due date	Priority	Status	Comments
Task 3(Lebo & Itumeleng) 1	L IM	Tomorrow		IN PROGRE...	
Task 2(Rio) 1	RG	Tomorrow		IN PROGRE...	
task 5(Junior ,Lebo & Itumeleng) 1	L MJ IM	Tomorrow		IN PROGRE...	
powerpoint presentation			High	IN PROGRE...	

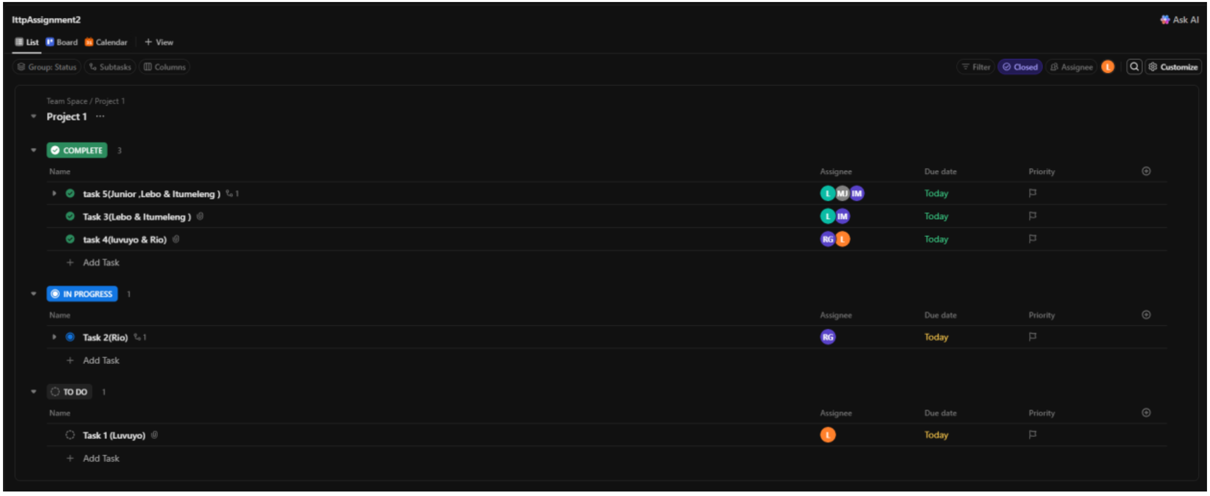
+ Add Task

TO DO 0

Name	Assignee	Due date	Priority	Status	Comments

+ Add Task

+ New status



Team Space / Project 1

Project 1 ···

COMPLETE 3

Name	Assignee	Due date	Priority
task 5(Junior ,Lebo & Itumeleng) 1	L MJ IM	Today	
Task 3(Lebo & Itumeleng)	L IM	Today	
task 4(luvuyo & Rio)	RG L	Today	

+ Add Task

IN PROGRESS 1

Name	Assignee	Due date	Priority
Task 2(Rio) 1	RG	Today	

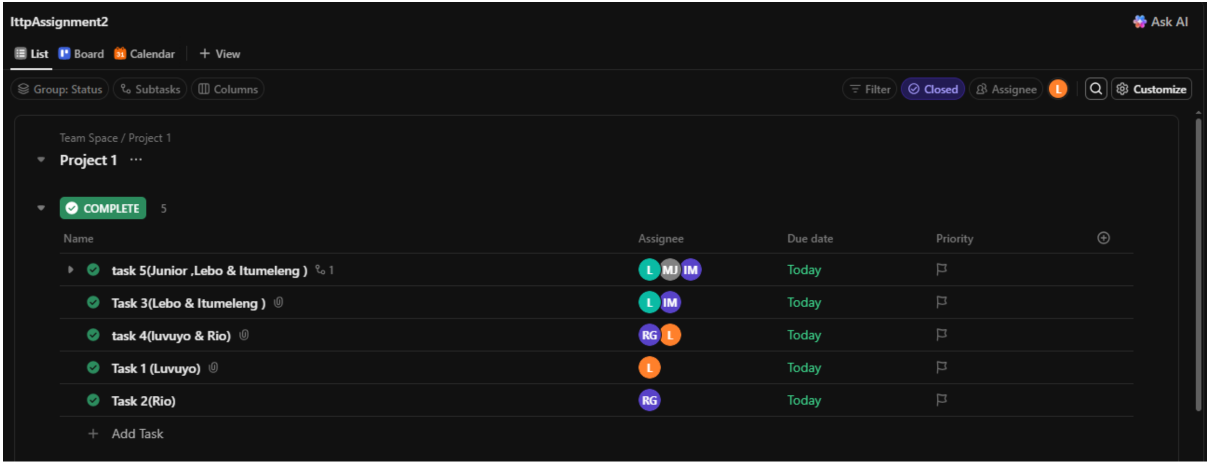
+ Add Task

TO DO 1

Name	Assignee	Due date	Priority
Task 1 (Luvuyo)	L	Today	

+ Add Task

Screenshots of when the tasks are complete:



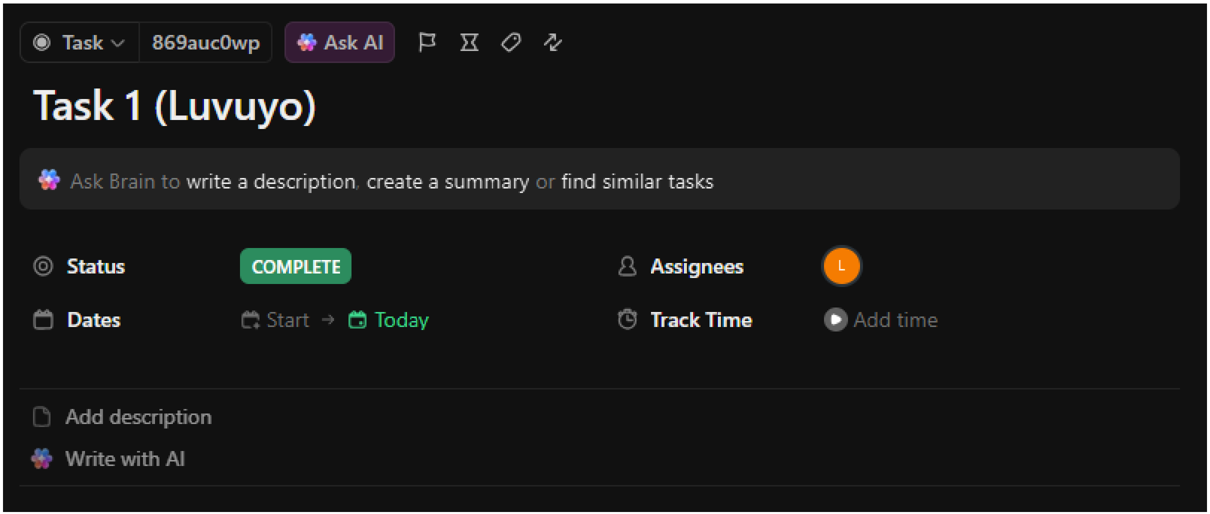
Team Space / Project 1

Project 1 ···

COMPLETE 5

Name	Assignee	Due date	Priority
task 5(Junior ,Lebo & Itumeleng) 1	L MJ IM	Today	
Task 3(Lebo & Itumeleng)	L IM	Today	
task 4(luvuyo & Rio)	RG L	Today	
Task 1 (Luvuyo)	L	Today	
Task 2(Rio)	RG	Today	

+ Add Task



Task 1 (Luvuyo)

Ask Brain to write a description, create a summary or find similar tasks

Status: COMPLETE

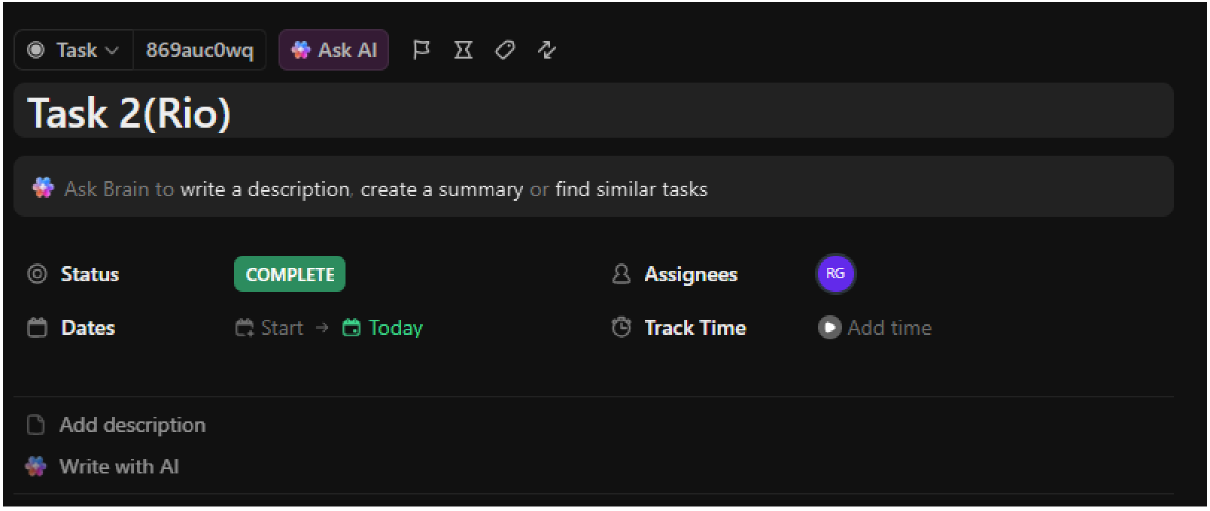
Assignees: L

Dates: Start → Today

Track Time: Add time

Add description

Write with AI



Task 2(Rio)

Ask Brain to write a description, create a summary or find similar tasks

Status: COMPLETE

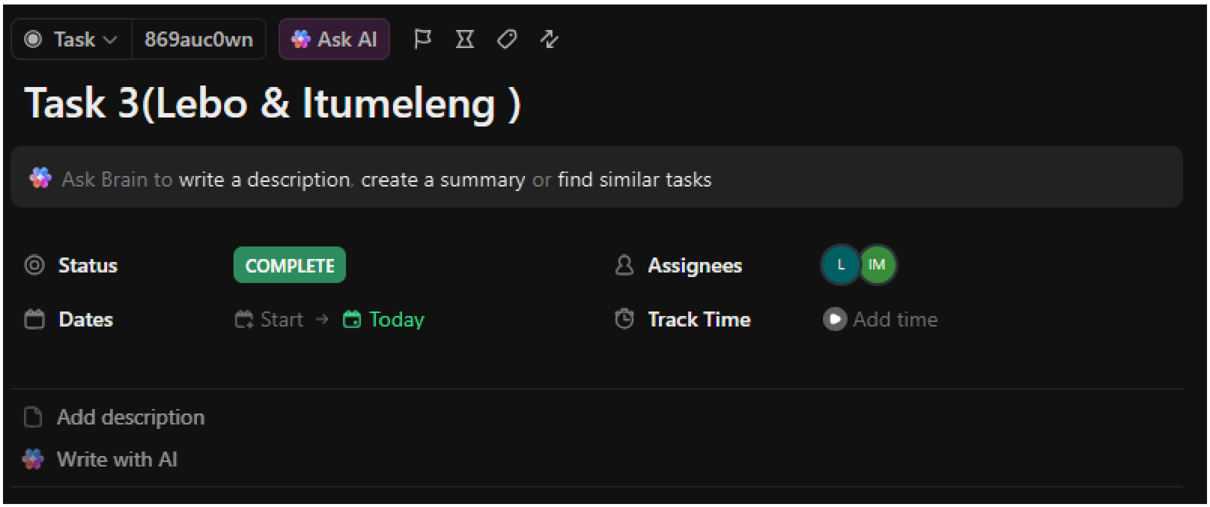
Assignees: RG

Dates: Start → Today

Track Time: Add time

Add description

Write with AI



Task 869auc0wn Ask AI

Task 3(Lebo & Itumeleng)

Ask Brain to write a description, create a summary or find similar tasks

Status: COMPLETE

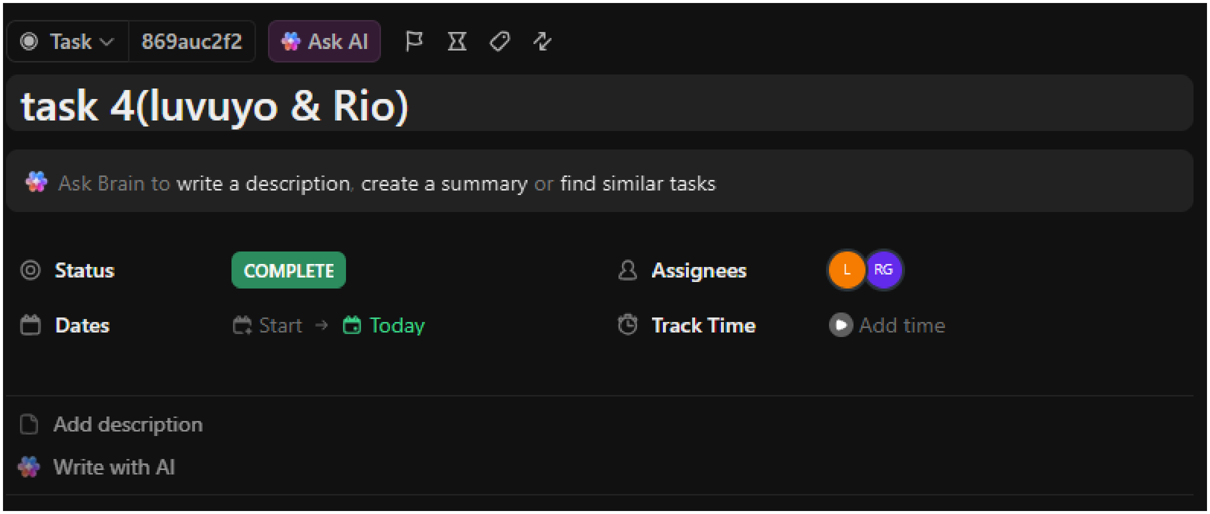
Assignees: L IM

Dates: Start → Today

Track Time: Add time

Add description

Write with AI



Task 869auc2f2 Ask AI

task 4(luvuyo & Rio)

Ask Brain to write a description, create a summary or find similar tasks

Status: COMPLETE

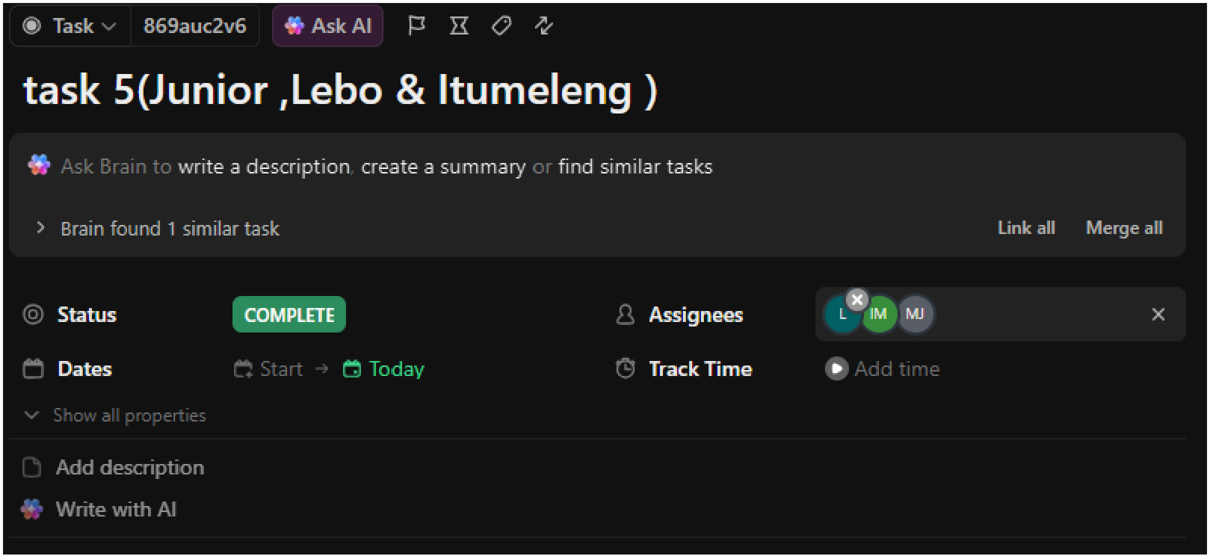
Assignees: L RG

Dates: Start → Today

Track Time: Add time

Add description

Write with AI



Task 869auc2v6 Ask AI

task 5(Junior ,Lebo & Itumeleng)

Ask Brain to write a description, create a summary or find similar tasks

Brain found 1 similar task Link all Merge all

Status: COMPLETE

Assignees: L IM MJ

Dates: Start → Today

Track Time: Add time

Show all properties

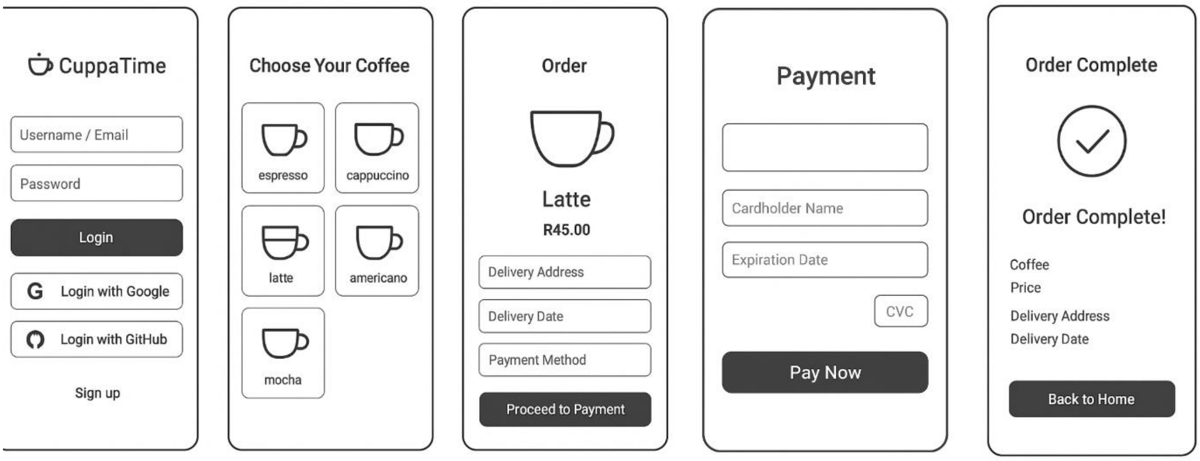
Add description

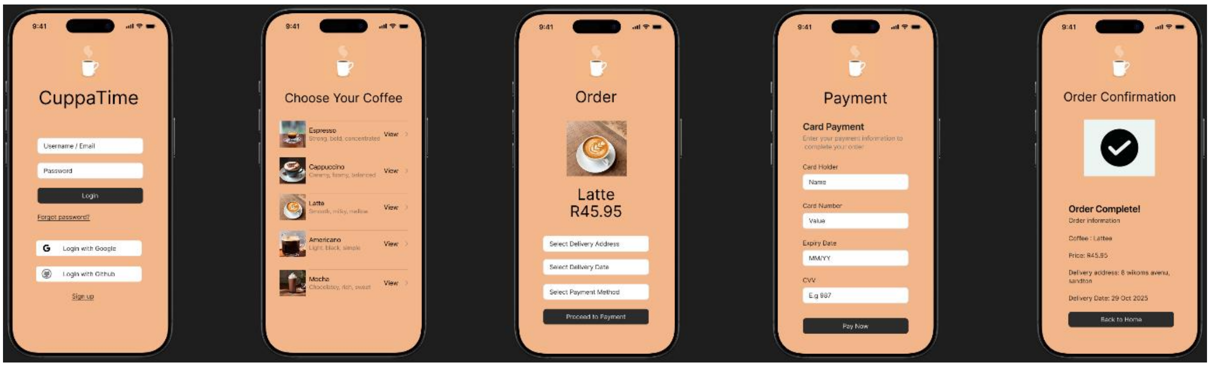
Write with AI

Link to the project on the project management tracking tool (ClickUp):

https://app.clickup.com/90121272035/v/l/7-90121272035-1 (The link may not work due to upgrading of Click Up subscription Payment)

Q1.2) Wireframe skeleton prototype, wireframe prototype app, screenshot and links to wireframes:





https://www.figma.com/design/XrCFDSxGIR57kSKxfEwT6F/CuppaTime-Skeleton-WireFrame-Q1.2-ITTP-Group-Assignment?m=auto&t=UdbKGBOQxwTxrnED-6

https://www.figma.com/design/2h3xVV5up6BoiUwAYXVJle/CuppaTime-Wireframe-prototype-app-Q1.2-ITTP-Group-Assignment?m=auto&t=9dy1hy8EckJHUdnx-6

Q1.3) Video presentation link:
https://youtu.be/6za4hJrwtHY

Q1.4) Copyright and licensing of our artefacts and software:
Licensing and Copyright Report for CuppaTime Prototype

1. Introduction

Intellectual property (IP) includes creations of the mind such as discoveries, innovations, designs, works of art etc. which are used in commerce. In IT terms, IP comprises source code, logos, interface styles and designs, written material texts and multimedia. Protecting IP gives creators control over who can use, distribute and even modify their creation.

2. Intellectual Property in Relation to CuppaTime

The cuppatime prototype is a unique digital artefact used to showcase the coffee ordering app. The prototype contains the following materials that constitute intellectual property: Software design and user interface (UI) The visual appearance such as layout, colour scheme and information hierarchy on the login, selection of services offered by and payment screens is a creative work.

Content and branding: CuppaTime is a brand, with a name (CuppaTime), logo and explanatory text. Code and functionality: The back-end logic of the app, form validation, and how the user interacts with a flow might be considered the original works under copyright law.

Interacting in combination, these features of the program represent a novel software product and warrant copyright protection.

3. Copyright Application

The work becomes automatically copyrighted when it is created and fixed in any tangible medium (including digital files). For the CuppaTime prototype, this means that its creator has become the sole owner of rights to reproduce, adapt, distribute and publicly display the app. Permission would nevertheless be needed to be granted for any 3rd party to download and reuse, or alter the design.

Be sure to remember that if your prototype has any third-party resources (like icons, fonts, or images), then they should be your own, free, or you have permission from the owner. Credit should be given for any borrowed content.

4. Licensing Choice

To provide a happy medium between ownership and educational/collaborative sharing, we will release the prototype under a CC BY-NC-SA license. This means others may inspect, use and modify the prototype for non-commercial purposes as long as they credit its creator, and license any derivative work based on it under the same terms. On the other hand, if the author wants to go commercial with CuppaTime, then a custom software license would make more sense: non-authorised use and distribution would be prohibited.

5. Conclusion

The CuppaTime prototype protects the creator's intellectual property while permitting controlled sharing or eventual commercialization through the use of copyright protection and a suitable license. In the IT industry, proper licensing also guarantees respect for creative ownership and ethical software development.

Question 2

Q2.1) Written proposal:

CyberGuard Solutions

Comprehensive Proposal to Address the Ransomware Attack on Netcare Waterfall City Hospital

1. Overview of 21st Century Fraud and Cybercrime

Every industry, including healthcare, has seen a significant digital transition in the twenty-first century. As a result of these developments, one of the biggest risks to data integrity, privacy, and business continuity is cybercrime. *(CISA, 2023; WHO, 2023; Europol, 2023)*.

Cybercriminals now frequently utilize ransomware, phishing, data breaches, and identity theft as attack vectors to take advantage of weaknesses in IT systems *(Kaspersky, 2024; Interpol, 2024)*. These attacks put lives at risk in the healthcare industry by disrupting vital medical procedures and compromising private patient data *(WHO, 2022; IBM Security, 2024)*.

Specifically, ransomware attacks lock an organization's data and demand payment for the decryption keys, which are frequently in cryptocurrency. This can lead to financial and reputational harm *(Europol, 2023; Kaspersky, 2024)*. A strong, safe, and well-coordinated cybersecurity system is desperately needed, as demonstrated by the recent ransomware outbreak at your hospital *(CISA, 2023; NIST, 2023)***.**

2. Our Function as Cybersecurity and IT Experts

Leading cybersecurity company CyberGuard Solutions focuses on long-term cyber resilience, digital forensics, and crisis response. Network engineers, forensic investigators, risk management experts, and cybersecurity analysts make up our team.

In dealing with this situation, our responsibilities include:

- Incident Response & Containment: To stop the ransomware threat from spreading further across systems and devices, it is imperative to promptly identify, isolate, and neutralize it *(CISA, 2023; CyberGuard Solutions, 2024)*.
- Data Restoration & Recovery: Restoring encrypted files with the least amount of interference to hospital operations possible using safe backups, decryption software, or data reconstruction *(NIST, 2023; CISA, 2023)*.
- System analysis and forensics: Identifying the ransomware attack's origin, methodology, and point of entry in order to stop it from happening again.
- Long-Term Cybersecurity Strategy Implementation: Creating a long-term cybersecurity framework that includes network hardening, personnel training, and threat monitoring.
- Compliance & Reporting: Making sure that every recovery and preventive plan complies with worldwide cybersecurity standards like ISO/IEC 27001 and national data protection legislation like POPIA (Protection of Personal Information Act) *(Department of Justice, 2021; South African Government, 2013; ISO, 2018)*.

Since our team has demonstrated expertise in handling cyber crises in vital industries like healthcare, finance, and government, we ought to be given this project. Our multidisciplinary strategy guarantees both quick recuperation and long-term resilience.

3. Cybersecurity Codes of Conduct and Ethical Considerations

Integrity and trust in cybersecurity activities are based on ethical behavior. Our strategy closely complies with the following moral standards and guidelines:

1. Confidentiality
   Protecting patient and hospital data from unwanted disclosure during and after recovery.
2. Integrity:
   Upholding truthfulness, openness, and precision in all correspondence, technical work, and reporting.
3. Professional Responsibility: Always acting in the patients' and hospital's best interests.
4. Non-Maleficence ("Do No Harm"):
   Making sure that no instruments, techniques, or protocols utilized in recovery undermine data or harm already-existing systems.
5. Respect for Professional Standards:
   Adherence to established organizations' rules of behavior, including: o The International Information System Security Certification Consortium (ISC) ² The Code of:
   - The Code of Ethics of the International Information System Security Certification Consortium ((ISC)², 2024).
   - The ACM Code of Professional Conduct and Ethics *(ACM, 2023)*.
   - Professional Ethics Standards of ISACA (ISACA, 2023).

These moral pledges guarantee that our solution satisfies both legal and ethical requirements.

4. Involved Stakeholders

Collaboration amongst multiple stakeholders is necessary for a ransomware situation to be resolved effectively. Among the principal players are:

Stakeholder	Role/Responsibility
Hospital Board of Directors	Board of Directors of the Hospital Making strategic decisions and approving security strategies and recovery funds.
IT Department	Department of Information Technology Implementing cybersecurity measures and coordinating technical aspects within.
Medical Staff	cooperation of the medical staff and observance of the new security procedures during system restoration.
Patients	Patients recipients of enhanced system dependability and data safety.
CyberGuard Solutions (External Cybersecurity Team)	The external cybersecurity team, CyberGuard Solutions Oversee long-term preventive, rehabilitation, and incident response plans.
Legal and Compliance Teams	Teams for Compliance and Law ensuring that all activities adhere to POPIA and other pertinent data protection laws (Department of Justice, 2021; South African Government, 2013).
Law Enforcement Agencies	Law Enforcement Organizations Cybercriminals are being investigated, and cooperation may lead to prosecution (SAPS, 2022; Interpol, 2024).

Insurance Providers	Insurance Companies Damage evaluation and cyber-insurance claim processing.

5. Overview of the Suggested Solution

Quick Reaction (First 72 Hours):

- Remove compromised systems from the network (CISA, 2023; NIST, 2023).
- Perform forensic analysis and malware containment quickly *(CyberGuard Solutions, 2024)*.
- Turn on data recovery with cloud or offline backups.
- Alert the appropriate cybersecurity response centers (CSIRT, for example) and legal authorities (Interpol, 2024; CISA, 2023).
- Communicate openly and honestly with employees and stakeholders.

Temporary Recuperation One to two weeks

- Restore vital systems, such as medical devices, appointment software, and patient records (Who, 2023).
- Use multi-factor authentication (MFA) and reset all user credentials (NIST, 2023).
- Perform vulnerability scanning throughout the entire network.
- Start training employees on cybersecurity awareness (ISO, 2018; WHO,2023).

Long-Term (Continuous) Prevention

- Implement endpoint security and a next-generation firewall (NIST, 2013; IBM Security, 2024).
- Put intrusion detection and continuous monitoring technologies into place(CISA, 2023).
- Plan frequent data backups and offsite secured storage.
- Provide every hospital staff with a Cybersecurity Policy Manual.
- Perform cybersecurity audits on a quarterly basis.

CyberGuard Solutions

Comprehensive Proposal to Address the Ransomware Attack on Netcare Waterfall City Hospital

6. Ransomware Attack Details and Loopholes

The current report did not explicitly say from which point of entry or how the ransomware specifically attacked Netcare Waterfall City Hospital.
Nor does it mean that the attack avenues typically exploited by online criminals and therefore the potential weak spots are:

- Ransomware itself.
- Phishing.
- Data breaches.
- Identity theft.

Such attacks are often perpetrated by cybercriminals who identify vulnerabilities in IT systems to stage the attack. Live system analysis and forensics, a core functionality of our proposed CyberGuard Solutions, would attempt to trace the attack back to its source, method of operation and point-of-entry *(SAPS, 2022; CyberGuard Solutions, 2024)*. Attack History Database – compile information regarding known attacks in order to try and prevent future occurrence.

7. Urgent Containment and Restoration Measures

Quick Reaction (First 72 Hours)

The Quick Reaction (First 72 Hours) plan involves the following immediate measures:

- Isolate systems that are known to be compromised.
- Carry out rapid forensic and malware containment.
- Enable data recovery including in cloud or offline backups.
- Inform the right CSIRT (Computer Security Incident Response Team, for example) and Legal entities.
- Be transparent with employees and stakeholders.

Temporary Deceleration (One to two weeks)

The following 1. Temporary Deceleration (One to two weeks) deals with recovery of basic functions:

- Bring back critical systems like medical equipment, scheduling software and patient files.
- Implement multi-factor authentication (MFA) and force users to reset their passwords.
- Conduct a full network vulnerability scan.
- Begin training employees in awareness of cyber security.

8. Ransomware Removal Without Paying and Safe Operations Techniques

Removing Ransomware Without Payment

Removing Ransomware Without Payment
The recommended plan focuses on Returning to Normal: Data Restoration & Recovery
Below is a chart showing comparisons of PCI Posture using the “pay or don’t pay” mix and alternate choices.

- Decrypting files using secure backups (cloud or offline)
- Utilizing decryption software.
- Data reconstruction.

This model will try to bring back files with minimization of hospital's operations' breakdowns.

Continuing Functioning Safely

To run safely while addressing the crisis, the hospital would depend on the following elements of both temporary and long-term plans:

- Incident Response & Containment: Detect, contain and terminate the threat to prevent it from spreading.

- Restore Critical Systems: Focus on restoring critical services such as medical devices, patient records, appointment software etc.
- Increased Security: Enable multi-factor authentication (MFA) and reset passwords.
- Personnel Cooperation: Gaining the cooperation of the staff and adherence to new security practices when restoring the system.

9. Effect of Removing Infected Systems

The plan's first step is to quarantine infected machines.

Potential for Harm: This will mean much needed medical treatment as well as others operations may be affected. Deactivating systems makes them unavailable, so the open can affect use of patient care and administrative services until the devices are cleaned and reactivated.

So What (The Rationale): This is critical for IR & Containment. It is designed to prevent the ransomware threat from spreading mechanisms on systems and devices. As intrusive as it sounds, this is essential to localizing the infection and preserving the integrity of your remaining network and data.

10. Rules and Policies for Prevention

The long-term cybersecurity strategy implementation and the long-term (pervasive) prevention plans prescribe rules, polices and even ethic and legal guidelines:

Technical and Operational Rules

- Long term Cyber security framework – A holistic framework which includes network hardening, training for employees and monitoring the threats.
- Security Implementation: Deploying endpoint security as well as next-gen firewall.
- Continuous Monitoring: Deploy intrusion detection and continuous monitoring tools.
- What They Do: Deciding how often to back up data and where to store the info.
- Policy & Audits: Quarterly Cybersecurity Audits and a Cybersecurity Policy Manual for every hospital employee.
- System Analysis – Constantly pinpointing the origins, method of attack and point of entry for the ransomware attack to ensure it doesn't return.

Ethical and Compliance Practices or Requirements

CyberGuard Solutions' approach is consistent with a number of ethical norms, law and industry regulation:

- Privacy: Maintaining the secrecy of patient and hospital information from being exposed, during and after recovery.
- INTEGRITY: Being truthful, transparent and accurate in all work and reports.
- Professional Obligations: At all times in patient's, and hospital's best interest.
- Non-Maleficence ("Do No Harm" Negagive): With nothing that the apprenticeships use to attack data or harm other systems.

- Legal Compliance: Ensuring all recovery and prevention plans conform to national data protection legislation, such as POPIA (Protection of Personal Information Act) *(Department of Justice, 2021; South African Government, 2013)*.
- International Standards Compliance: Complying with global cybersecurity standards such as ISO/IEC 27001 *(ISO, 2018)*.

Professional Conduct Codes

Compliance with established associations' standards of conduct, which may include:

- **The ISC's Code of Ethics**, contained in the Certified Information System Security Professional exam, itemizes: *The Code of Ethics for the International Information System Security Certification Consortium (ISC)²* is a testament to their commitment to their members.
- **The ACM Code of Professional Conduct and Professional Ethics.**
- **Professional Ethics Standards of ISACA.**

Overview of the Suggested Solution

Quick Reaction (First 72 Hours):

- Isolate systems that are known to be compromised.
- Carry out rapid forensic and malware containment.
- Enable data recovery including in cloud or offline backups.
- Inform the right CSIRT (Computer Security Incident Response Team, for example) and Legal entities.
- Be transparent with employees and stakeholders.

Temporary Recuperation One to two weeks

- Bring back critical systems like medical equipment, scheduling software and patient files.
- Implement multi-factor authentication (MFA) and force users to reset their passwords.
- Conduct a full network vulnerability scan.
- Begin training employees in awareness of cyber security.

Long-Term (Continuous) Prevention

- Implement endpoint security and a next-generation firewall.
- Put intrusion detection and continuous monitoring technologies into place.
- Plan frequent data backups and offsite secured storage.
- Provide every hospital staff with a Cybersecurity Policy Manual.
- Perform cybersecurity audits on a quarterly basis.

Q2.2)
Presentation is provided on arc under this documentation.

Question 3

Peer evaluation of all group members is provided on arc under this documentation.

Reference

Association for Computing Machinery (ACM). (2022) *ACM Code of Ethics and Professional Conduct*. Available at: https://www.acm.org/code-of-ethics (Accessed: 15 October 2025).

Association for Computing Machinery (ACM). (2023) *ACM Code of Ethics and Professional Conduct*. Available at: https://ethics.acm.org (Accessed: 14 October 2025).

Creative Commons (n.d.) About the licenses. Available at: https://creativecommons.org/licenses/ (Accessed: 15 October 2025).

CyberGuard Solutions. (2024) *Incident Response and Forensic Analysis Framework*. Johannesburg: CyberGuard Internal Security Proposal.

Cybersecurity and Infrastructure Security Agency (CISA). (2023) *Ransomware Guide: Prevention, Response, and Recovery*. U.S. Department of Homeland Security. Available at: https://www.cisa.gov/stopransomware (Accessed: 15 October 2025).

Department of Justice (South Africa). (2021) *Protection of Personal Information Act (POPIA)*. *Government Gazette*, Republic of South Africa.

Europol. (2023) *Internet Organised Crime Threat Assessment (IOCTA 2023)*. Available at: https://www.europol.europa.eu (Accessed: 14 October 2025).

Figma. (2023) Available at: https://www.figma.com/files/team/1403118862158530800/recents-and-sharing?fuid=1402623545477273363

Figma (2023) *Figma*. Available at: https://www.figma.com/files/team/1403118862158530800/recents-and-sharing?fuid=1402623545477273363 (Accessed: 15 October 2025).

Government of South Africa (n.d.) Copyright Act 98 of 1978. Available at: https://www.gov.za/documents/copyright-act (Accessed: 15 October 2025).

IBM Security. (2024) *Cost of a Data Breach Report 2024*. Available at: https://www.ibm.com/reports/data-breach (Accessed: 14 October 2025).

Information Systems Audit and Control Association (ISACA). (2023) *Code of Professional Ethics*. Available at: https://www.isaca.org (Accessed: 14 October 2025).

International Intellectual Property Alliance (IIPA) (n.d.) Understanding copyright and related rights. Available at: https://iipa.org/ (Accessed: 15 October 2025).

Information Systems Audit and Control Association (ISACA). (2023) *Code of Professional Ethics*. Available at: https://www.isaca.org (Accessed: 15 October 2025).

International Information System Security Certification Consortium ((ISC)²). (2024) *Code of Ethics*. Available at: https://www.isc2.org/Ethics (Accessed: 14 October 2025).

International Organization for Standardization (ISO). (2018) *ISO/IEC 27001:2018 Information Security Management Systems – Requirements*. Geneva: ISO.

Interpol. (2024) *Ransomware: How It Works and How to Protect Yourself*. Available at: https://www.interpol.int/en/Crimes/Cybercrime/Ransomware (Accessed: 14 October 2025).

Kaspersky. (2024) *Ransomware Explained*. Available at: https://www.kaspersky.com/resource-center/threats/ransomware (Accessed: 14 October 2025).

National Institute of Standards and Technology (NIST). (2023) *Framework for Improving Critical Infrastructure Cybersecurity*, Version 2.0. Available at: https://www.nist.gov/cyberframework (Accessed: 14 October 2025).

South African Department of Trade, Industry and Competition (DTIC) (n.d.) Intellectual property policy of the Republic of South Africa. Available at: https://www.thedtic.gov.za/ (Accessed: 15 October 2025).

South African Government. (2013) *Protection of Personal Information Act 4 of 2013 (POPIA)*. Available at: https://www.gov.za/documents/protection-personal-information-act (Accessed: 14 October 2025).

South African Police Service (SAPS). (2022) *Cybercrime and Digital Forensics Investigations*. Pretoria: SAPS Cyber Unit.

World Intellectual Property Organization (WIPO) (n.d.) What is intellectual property? Available at: https://www.wipo.int/about-ip/en/ (Accessed: 15 October 2025).

World Health Organization (WHO). (2022) *Cybersecurity in the Health Sector*. Available at: https://www.who.int/publications (Accessed: 14 October 2025).

World Health Organization (WHO). (2023) *Cybersecurity for Health Facilities: Ransomware and Data Protection Guidance*. Geneva: WHO Publications.

World Intellectual Property Organization (WIPO) (n.d.) Copyright basics. Available at: https://www.wipo.int/copyright/en/ (Accessed: 15 October 2025).