Q1.4 Copyright and Licensing of My Prototype

Intellectual Property (IP) refers to creations of the human mind such as inventions, designs, artistic works, software, and digital content that are legally protected through different rights. These include copyrights, trademarks, patents, industrial designs, and trade secrets. IP makes sure that creators can benefit from their original work while preventing unauthorized use or reproduction. In South Africa, IP is protected under multiple laws including the Copyright Act 98 of 1978, and international agreements such as the Berne Convention, TRIPS, and WIPO treaties.

For our prototype; a mobile coffee-ordering application designed in Figma, intellectual property applies to both the visual design and functional concept of the app. The layout, icons, color schemes, and interface design qualify as artistic works under copyright law, while the written content (such as button labels or descriptions) qualifies as literary works. Should the app progress into a coded version, the source code would be classified as a computer program, also protected as a literary work under the South African Copyright Act.

By owning this prototype, We automatically obtain copyright protection now of creation. This means others cannot copy, modify, or distribute our design without permission. The prototype was developed collaboratively, thus copyright ownership is shared among us the contributors, as collaborative works are co-owned by their authors.

To ensure proper legal and ethical use, We applied the MIT License to this prototype when publishing it on GitHub. The MIT License is an open-source license that allows others to use, copy, modify, and distribute the software freely, if they give appropriate credit to the original author. This promotes innovation and sharing while maintaining recognition for our work. In Figma, We can also include a short notice indicating “© 2025 [LL Rantsane, Monde, Yamikani, Katleho ] – Licensed under MIT License” to remind users of the terms.

Additionally, We must respect the copyright of others by not using copyrighted icons, images, or fonts without permission. Any third-party assets used must be under open or royalty-free licenses such as Creative Commons.

In conclusion, intellectual property safeguards creative and technical efforts like my Figma prototype. By applying the MIT License and adhering to copyright laws, We maintain ownership while allowing open collaboration in a legally protected manner.

**Reference List (APA 7th edition)**

1. Rosebank College. (2025). *ITPP5112/p/w Module Manual 2025*. Rosebank College.
2. Figma. (n.d.). *Figma: Collaborative interface design tool*. Retrieved October 23, 2025, from <https://www.figma.com>
3. GitHub. (n.d.). *GitHub: Where the world builds software*. Retrieved October 23, 2025, from <https://github.com>

# **Question2**

1. COMPANY PROFILE

SecureMed Guardian is a South-African-owned cyber-security firm registered 2017, staffed by 42 professionals (12 CISSPs, 8 CISM, 6 GIAC, 4 medical-device security specialists, 3 attorneys). We hold:

* ISO/IEC 27001:2022 certification
* ISETA & HPCSA-accredited training provider
* Level-1 B-BBEE contributor
* Professional indemnity (ZAR 50 m) & cyber-liability cover.

1. INTRODUCTION – CYBER-CRIME & FRAUD LANDSCAPE

* 2024 Verizon DBIR: 28 % of all ransomware incidents occurred in health-care.
* Average downtime = 19 days; average cost = USD 10.93 m.
* Double-extortion (data theft + encryption) used in 77 % of cases.
* Regulatory fines under GDPR / POPIA can reach 4 % of annual turnover.
* Reputational damage causes permanent loss of donor & patient trust.

1. OUR ROLE AS IT PROFESSIONALS

We apply the triad:

1. PREVENT – reduce attack surface.
2. DETECT – discover anomalies in seconds.
3. RESPOND – contain, eradicate, recover ethically & lawfully.  
   Our multi-disciplinary team (network engineers, penetration testers, digital-forensics analysts, medical-device auditors, privacy attorneys) aligns with:

* NIST SP 800-66 Rev.2 (HIPAA)
* ISO 27799:2016 (health informatics)
* HISA-SA Clinical Risk Management Guideline 2023
* King IV Report on Corporate Governance.

1. ETHICAL ELEMENTS & CODES OF CONDUCT

We subscribe to:

* ACM Code of Ethics – avoidance of harm, honesty, confidentiality.
* BCS Code – integrity, professionalism, respect privacy, continuing development.
* EC-Council C|EH “Do no harm” clause.
* HPCSA “e-Health” guidelines – patient safety is primus inter pares.  
  Internal enforcement: quarterly ethics review, whistle-blower hotline, mandatory 20 CPE hours/year on privacy & ethics.

1. STAKEHOLDER MATRIX

Stakeholder | Interest | Our Communication Mode  
Board / Exec | Liability & reputation | Weekly status deck & risk register  
Clinicians | Continuity of care | Downtime SOP cards, 24 h phone bridge  
Patients | Safety & privacy | Public website updates (GDPR Art.12)  
Regulators | Compliance evidence | Structured breach notification files  
Insurers | Claim validity | Forensic chain-of-custody reports  
Suppliers | Device integrity | Coordinated vendor patching window  
Media / Public | Trust | Single appointed spokesperson; factual, no blame.

1. ATTACK VECTOR ANALYSIS – HOW RANSOMWARE ENTERED

Forensic timeline (confirmed via log correlation & EDR telemetry):

1. 03 Oct 09:14 – Spear-phishing e-mail to radiology clerk spoofing “PACS update”.
2. 03 Oct 09:27 – Macro enabled → Cobalt-Strike beacon to 185.220.x.x.
3. 03 Oct 10:05 – Credential harvesting → obtained service account “PACSsvc”.
4. 03 Oct – 07 Oct – Lateral movement; discovered flat network; escalated to Domain Admin.
5. 08 Oct 02:11 – Deployment of “LockHeal\_v4.2” ransomware via GPO; MBR & VSS destroyed.

Root loopholes

* No MFA on Outlook Web Access.
* Flat network (office & biomedical same VLAN).
* SMBv1 enabled on legacy Windows 7 imaging boxes.
* Excessive service-account privileges.
* EDR not installed on 38 % of workstations.
* Backups accessible via domain credentials; no offline copy.

1. IMMEDIATE CONTAINMENT ACTIONS (FIRST 72 h)
2. Incident declared – Crisis Command Centre activated.
3. Network segmentation – core uplinks disconnected; life-critical VLAN isolated.
4. Life-support devices kept powered but monitored locally – no remote shutdown.
5. Snapshot forensic images captured (SHA-256 verified).
6. Malicious IPs & domains sink-holed via ISP.
7. Compromised accounts disabled; krbtgt password reset 2×.
8. Print daily clinical abstracts → paper fallback kits distributed to wards.
9. Regulator & patient notification initiated (within 72 h POPIA window).
10. PR & staff comms – single source of truth; empathy tone; no ransom promise.
11. STRATEGY TO REMOVE RANSOMWARE WITHOUT PAYING

A. Clean slate rebuild

* Deploy parallel “green” Active Directory forest on new hardware.
* Re-image endpoints using gold-image library (SHA-2 verified).  
  B. Restore data
* Retrieve last offline backup (01 Oct) from LTO-9 WORM tapes stored off-site.
* Incremental replay of HL7 & DICOM messages from encrypted courier USB logs.  
  C. Validate integrity
* File-hash comparison against pre-incident checksums; any mismatch → quarantine.  
  D. Decryption fallback
* Checked NoMoreRansom & vendor intel – no free decryptor for LockHeal\_v4.2; therefore continue rebuild rather than pay.  
  E. Continuous monitoring
* Roll-out EDR (CrowdStrike) to 100 % endpoints; 24 h MDR service back-stopped by our SOC.

1. BUSINESS CONTINUITY WHILE RESOLVING CRISIS

* Elective surgeries postponed; emergency & trauma services maintained using paper + voice.
* Radiology: portable US & CR machines with local storage; films printed.
* Laboratory: critical results telephoned; non-urgent samples redirected to partner lab.
* Pharmacy: revert to paper prescriptions; dual-sign for narcotics.
* Patient administration: coloured wrist-bands for ID; Excel sheets on standalone PC.
* Daily situation report to Board at 18:00; clinical governance lead signs off on safety.

1. LONG-TERM PREVENTION PROGRAMME
2. Zero-Trust Architecture – micro-segmentation, 802.1X NAC, MFA every user & vendor.
3. Privileged Access Workstations (PAW) – separate admin tier, no Internet.
4. Patch-management SLA – critical within 7 days; medical devices via manufacturer coordinated disclosure.
5. Backup 3-2-1-1-0 regime – 3 copies, 2 media, 1 off-site, 1 offline, 0 backup-errors.
6. Security awareness – quarterly phishing simulations; target click-rate < 5 %.
7. Incident-response retainer – 24/7 SLA 2 h on-site; annual tabletop with clinicians.
8. Supply-chain security – security addendum in all procurement; right-to-audit clause.
9. Continuous compliance audits – ISO 27001 + 27799 re-certification every 3 years.
10. Ethics & governance board – any new monitoring technology requires human-rights & privacy impact assessment.
11. PROJECT TIMELINE & BUDGET (ZAR)

Phase | Duration | Cost  
Assessment & containment | 0 – 2 weeks | 1.2 m  
Rebuild & hardening | 2 – 8 weeks | 4.5 m  
Monitoring & training (Yr 1) | ongoing | 1.8 m  
Contingency (10 %) | — | 0.75 m  
TOTAL | 9 weeks + Yr 1 SOC | 8.25 m

ROI: avoided downtime cost (19 d × ZAR 6 m/d) ≈ 114 m → 14× return.

1. CONCLUSION & CALL TO ACTION

SecureMed Guardian possesses the technical competence, ethical foundation and health-sector experience to return [Hospital] to full operational capacity within 8 weeks while embedding a defensible, compliant and patient-safe cyber-resilience posture. We respectfully request the Board’s approval to proceed with the programme as outlined.