TM260 IT Ethics & Security – Study Guide (Chapters 1–3)

Chapter 1 – Introduction to IT Ethics

- Ethics = principles that govern right and wrong behavior in IT.
- Difference: Legal ≠ Ethical.
- Ethical Theories: Utilitarianism (greatest good), Deontology (duty-based), Virtue Ethics (character-based).
- Common dilemmas: plagiarism, piracy, hacking, misuse of data.
- Codes of Conduct: ACM, IEEE guidelines for IT professionals.

Chapter 2 – Privacy, Security, and Intellectual Property

- Privacy: right to control personal data (cookies, surveillance, big data risks).
- Security: CIA Triad – Confidentiality, Integrity, Availability.
- Privacy vs Security: Privacy = rights, Security = protections.
- Intellectual Property: copyrights, patents, trademarks, trade secrets.
- Violations: piracy, plagiarism, unfair use.
- Example: Company misuse of data, pirated software, copy-pasted code.

Chapter 3 – Cybercrime, Cybersecurity, and Society

- Cybercrime types: hacking, phishing, identity theft, malware, cyberbullying.
- Cyberterrorism: threats to national security and infrastructure.
- Laws: GCC/Kuwait cybercrime laws punish unauthorized access & misuse.
- Social impact: financial loss, misinformation, addiction, online fraud.
- Preventive measures: firewalls, antivirus, encryption, awareness.

■ Exam/TMA Tips

- Be ready to contrast ethical vs. legal issues.
- Always relate to CIA Triad & privacy/IP principles.
- Use real-world examples: Cambridge Analytica (privacy), WannaCry ransomware (cybercrime).