INTERNATIONAL UNIVERSITY OF EAST AFRICA
'Learning to Succeed'

FACULTY OF SCIENCE AND TECHNOLOGY

END OF SEMESTER EXAMINATIONS - DECEMBER 2025

PROGRAMME: MIT
YEAR/SEM: YEAR 1/SEMESTER 1
COURSE CODE: MIT717
NAME: CYBER LAW AND IT ETHICS

DATE:
TIME:

INSTRUCTIONS TO CANDIDATES:

SECTION A

Attempt One Question from Section A

Question 1:

QUESTION ONE (40 MARKS)

i. Differentiate between Computer Ethics and Cyberethics. (02 Marks)

ii. Explain how emerging technologies such as artificial intelligence, digital surveillance, and big data analytics introduce new ethical dilemmas in cyberspace. Provide relevant examples. (04 Marks)

iii. Identify and briefly explain four professional responsibilities expected of ICT practitioners in ensuring ethical behaviour within organisations. (08 Marks)

iv. Laws governing ICT can be categorised into Substantive Law and Procedural Law. Distinguish between these two categories and give one ICT-related example for each.
(04 Marks)

v. Professional codes of conduct play a major role in guiding ICT practitioners. Outline four key principles that should form the foundation of any ICT professional code of conduct.
(04 Marks)

vi. The growth of digital communication platforms has created an environment where cybercrime and unethical online behaviour continue to flourish.

a. Discuss the meaning of the following cyber-related offences, giving appropriate examples: (06 Marks)

-Identity theft

-Phishing

-Cyberbullying

b. Unauthorized access b. Propose four practical measures that governments, organisations, or individuals can implement to minimise cybercrime and promote ethical digital behaviour.
(08 Marks)

Question 2:

QUESTION TWO (40 MARKS)

i. Differentiate between law, morality, and ethics, and explain how they relate yet differ in

regulating human behaviour. (4 Marks)

ii. Explain the differences between civil law and criminal law, including examples of cases handled under each. (4 Marks)

iii. Describe the role of legislatures in establishing laws and explain why ethical principles are not created through the same process. (4 Marks)

iv. Define intellectual property (IP) and explain how intellectual property rights (IPR) protect creative and innovative works, giving examples. (4 Marks)

v. Distinguish between patents, copyrights, and trademarks, explaining what each protects and how they differ. (4 Marks)

vi. Explain the concepts of cyberpiracy, cybersquatting, and metatagging, and describe how each can be used to exploit trademarks online. (4 Marks)

vii. Explain the importance of clearly stated terms and conditions on an e-commerce website and how they affect online consumer protection. (4 Marks)

viii. Define the security principles of confidentiality, integrity, and interception, providing examples of how each may be protected or violated. (4 Marks)

ix. Describe the security threats of fabrication, spoofing, and phishing, explaining how attackers use them to compromise systems. (4 Marks)

x. Define computer crime and cybercrime, and give examples demonstrating the difference between the two. (4 Marks)

xi. Explain the differences between civil-law issues (such as contractual disputes) and cyber offences (such as cyberbullying or stalking). (4 Marks)

xii. Explain Denial of Service (DoS) attacks, describing their effects and how organisations can mitigate them. (4 Marks)

xiii. Identify and explain three common ethical issues IT users must avoid, such as piracy, misuse of resources, and inappropriate information sharing. (4 Marks)

xiv. Define email spamming and email spoofing, and explain why they pose ethical and security threats. (4 Marks)

xv. Explain what is meant by good morals, and provide examples of moral behaviour expected in a digital environment. (4 Marks)

xvi. Describe the importance of integrity, responsibility, and accountability in demonstrating IT professionalism in the workplace. (4 Marks)

xvii. Explain the functions of an IT professional body, and discuss why such bodies guide practice but do not enforce criminal punishments. (4 Marks)

xviii. Explain why regular antivirus updates, firewalls, and system patches are essential for safeguarding organisational computing resources. (4 Marks)

xix. Describe major challenges associated with licensing IT professionals, including lack of a standard body of knowledge or regulating authority. (4 Marks)

xx. Define a security policy, explain its purpose in an organisation, and describe how it protects users and assets. (4 Marks)

SECTION B

Attempt any Three Questions from Section B

Question 1:

QUESTION THREE (15 MARKS)

CASE STUDY: CONFIDENTIAL INFORMATION (12 MARKS)

Meditech Solutions Ltd is a company that manufactures hospital information systems used for patient registration, billing, and electronic medical records. The company has a long-standing technical flaw in its billing engine that occasionally fails to record insurance co-payments during peak transaction periods. As a workaround, clients are instructed to run a weekly reconciliation report to confirm billing accuracy.

John was previously the Senior Software Quality Engineer at Meditech Solutions. During his employment, he repeatedly warned management about the flaw and advised that it required a complete redesign of the billing engine. Management declined, citing budget constraints.

John later joined Helix Digital Health, one of Meditech's strongest competitors. In recent months, Meditech's sales team has noticed that hospital procurement teams especially in bids where they compete directly with Helix—have begun asking very specific questions about the reliability of Meditech's billing engine and how it handles missed co-payments. Under pressure, Meditech's sales teams have had to disclose the flaw, resulting in the loss of several contracts to Helix.

Meditech now wishes to sue John for breach of confidentiality. Explain what Meditech must demonstrate in order to succeed in court, and justify your reasoning.

Case Study: Copyright / Trademark / Software Piracy (8 Marks)
PixelForge Studios is a small Ugandan mobile-game development company with 15 employees. Its most successful game, JungleQuest, is published and distributed by ApexPlay Ltd, which owns the trademark and packaging rights for the game.

Two senior developers from PixelForge Samuel and Tricia resigned last year and joined Nova Interactive, a much larger game studio. Recently, Nova released a new game called SafariQuest, published by Arcadia Entertainment, one of ApexPlay's major competitors. SafariQuest features nearly identical gameplay mechanics, character progression systems, and storyline elements that strongly resemble JungleQuest. It is also sold at a lower price and its packaging, colour palette, and font designs are highly similar.

PixelForge Studios and ApexPlay believe that their intellectual property has been copied and want to take legal action. Explain which legal actions PixelForge and ApexPlay can take against Samuel, Tricia, Nova Interactive, and Arcadia Entertainment. Provide justification for each action and discuss why these actions might succeed in court.

Question 2:

QUESTION FOUR (20 MARKS)

Case Study: Cybersecurity Risks at Eastland University

Eastland University recently implemented a new online student information system (SIS) that handles admissions, registration, results, payments, staff management, and learning materials. The system is integrated with the university website, email platform, and an internal cloud-based storage system.

A recent internal audit revealed several security problems: staff were sharing passwords, many computers had outdated antivirus software, the university Wi-Fi had weak encryption, and some departments were still storing sensitive student data on unsecured personal laptops.

In the last two months, the university has experienced suspicious activities including: unknown users attempting to access the SIS login page at night, ransomware emails sent to staff, modification of student financial records, and two cases where attackers tried to intercept student transcripts emailed to employers.

Eastland University wants to strengthen its cybersecurity posture and better understand its threats, vulnerabilities, and attack exposure.

i. Distinguish between threats and vulnerabilities in the context of Eastland University's cyber environment. Provide clear explanations showing how the two concepts relate to cybercrimes. (08 Marks)

ii. Identify and explain any three vulnerabilities present in Eastland University's systems, based on the case study. For each vulnerability, describe how it can be exploited by cybercriminals. (06 Marks)

iii. Using examples relevant to Eastland University, explain the four categories of cyber threats interception, interruption, modification, and fabrication. (06 Marks)

Question 3:

QUESTION FIVE (20 MARKS)

Case Study: Cybersecurity Challenges at Horizon Microfinance Bank

Horizon Microfinance Bank recently migrated its loan processing, customer onboarding, and mobile banking services to a new cloud-based digital platform. While the new system has improved customer convenience, an internal audit revealed several weaknesses: staff frequently use weak passwords, some customer data is stored in unencrypted form, and the mobile banking API has no rate-limiting, leading to multiple failed login attempts from unknown IP addresses.

Recently, Horizon experienced disruptions including delayed loan approvals due to server

downtime, unauthorized attempts to view customer credit files, and corruption of transaction logs after a system update. Management now wants to understand the implications of these incidents and how to strengthen the CIA triad.

i. Three concepts—Confidentiality, Integrity, and Availability—are central to cybersecurity. Explain at least three kinds of harm Horizon Microfinance Bank might experience when any part of its CIA triad is compromised. (09 Marks)

ii. Preserving confidentiality, integrity, and availability of information systems relates closely to the threats of interruption, interception, modification, and fabrication. Explain how each of the CIA components corresponds to, overlaps with, or is affected by these four threat categories. (06 Marks)

iii. A control is an action, device, procedure, or technique that reduces or removes vulnerabilities. Describe several types of controls that Horizon Microfinance Bank could implement to protect its systems, giving examples in each case. (05 Marks)

Question 4:

QUESTION SIX (20 MARKS)

Case Study: Digital Content Protection at EduVision Learning Platform

EduVision is a rapidly growing online learning platform offering digital textbooks, video lectures, and interactive coding labs. The company invests heavily in producing high-quality digital content and licensing learning materials from international publishers. Recently, EduVision discovered that some of its premium e-books and video tutorials were being illegally shared on social media groups, student WhatsApp groups, and unauthorized file-sharing websites. The company also receives frequent complaints from users who do not understand the platform’s terms of service, especially regarding payment refunds, digital rights, and the use of cookies for analytics. EduVision now wants to strengthen its legal protection, improve user awareness, and minimise misuse of its digital assets.

i. Copyrights and patents are important mechanisms for protecting intellectual property. Describe the purpose of each and explain how EduVision can use these forms of protection to safeguard its digital learning innovations. (04 Marks)

ii. Explain why it is necessary for EduVision to clearly display terms and conditions of purchase on its e-commerce platform. (04 Marks)

iii. Explain why EduVision must include a cookie-use disclaimer to inform users that their browsing data may be collected when using the platform. (04 Marks)

iv. Software piracy remains a major ethical dilemma: EduVision loses revenue when its paid content is shared illegally, yet many learners cannot afford premium subscriptions. As a student of IT ethics, discuss this dilemma and provide a reasoned opinion on how EduVision could balance intellectual property protection with accessibility and affordability. (08 Marks)

Question 5:

QUESTION SEVEN (20 MARKS)

Case Study: Professionalization Challenges in the Uganda Data Science Association (UDSA)

The Uganda Data Science Association (UDSA) is a newly formed organisation aiming to professionalise the work of data analysts, data engineers, machine-learning specialists, and AI practitioners across the country. UDSA hopes to establish minimum training standards, certify practitioners, promote ethical use of data, and advocate for responsible AI.

However, the association faces challenges: many practitioners work without formal certification, employers rarely require membership in a professional body, and the public lacks awareness of professional standards in data science. UDSA leadership is therefore exploring how to strengthen professionalism, clarify roles, and promote ethical conduct in the industry.

i. Write short notes about the following: (06 Marks)

a. Professional Employees

b. A Professional Piece

c. A Professional Body

ii. As a professional body matures, it typically develops several important functions. Discuss any three such functions in relation to UDSA. (04 Marks)

iii. All professional bodies establish a code of conduct/ethics that members must follow. Write short notes on the following ethical principles: (06 Marks)

a) The Public Interest

b) Duty to the Relevant Authority

c) Duty to the Profession

d) Professional Competence and Integrity

iv. In many developing countries, the establishment of IT and data-related professional bodies is still uncommon. Using a SWOT analysis, discuss whether creating a professional body like UDSA is compelling in your home country. (04 Marks)

Question 6:

QUESTION EIGHT (20 MARKS)

Case Study: Cyberethics Challenges at DigiMarket Africa

DigiMarket Africa is a fast-growing e-commerce and social-interaction platform used by millions across several African countries. The platform allows users to post products, communicate through private messages, join discussion groups, and make digital payments. However, the company has noticed rising incidents of unethical online behaviour: anonymous users sending threatening messages, fake seller accounts scamming buyers, cases of

cyberstalking targeting female sellers, and reports that some users are sharing harmful or illegal digital content through private groups.

The management of DigiMarket Africa is increasingly concerned about the lack of strong cyberethics awareness among users, the absence of effective enforcement mechanisms, and limited public understanding of online rights and responsibilities. The company now wants to strengthen its cyberethics framework, improve user protection, and reduce online abuse.

i. Among the unethical issues that can arise on digital platforms are cyberstalking, cyber harassment, electronic fraud, and the distribution of prohibited or harmful digital content. Explain what each of these terms means and provide examples relevant to the DigiMarket Africa scenario. **(08 Marks)**

ii. Discuss practical remedies that DigiMarket Africa and similar platforms can put in place to reduce cybercrime and unethical online behaviour. Your discussion may include policy, legal, technical, organisational, and user-awareness measures. **(12 Marks)**

Question 7:

QUESTION NINE (20 MARKS)

Case Study: Network Security Audit at GreenLeaf Medical Center

You are a cybersecurity analyst hired to conduct a network-security audit for GreenLeaf Medical Center, a private hospital that stores thousands of sensitive patient records, laboratory results, and electronic prescriptions. During your assessment, you discover that the hospital's wireless network is using outdated security protocols, allowing unauthorized individuals within the vicinity to potentially intercept patient data. You also find that staff frequently share Wi-Fi passwords with visitors and external contractors.

When you report this vulnerability to the IT Manager, they dismiss your concerns, saying that upgrading the wireless infrastructure and implementing secure authentication would be too costly and would disrupt hospital operations. The manager instructs you to finalize the audit report without mentioning the wireless-security issue.

You now face an ethical and professional dilemma regarding how to proceed.

i. What should you do in response to the IT Manager's instruction? (06 Marks)

ii. Explain your response with reference to the potential consequences of ignoring or concealing the identified security risk. (06 Marks)

iii. Explain your response with reference to your professional responsibilities, ethical considerations, and obligations as a cybersecurity practitioner. (08 Marks)

Question 8:

QUESTION TEN (20 MARKS)

Case Study: Bias Concerns in an AI-Powered Recruitment System

TalentPlus Innovations is developing an AI-powered recruitment system intended to automate candidate screening and improve hiring efficiency for large organisations. During the system's pilot testing, you discover that the model consistently ranks applicants from certain rural regions lower than equally qualified candidates from urban areas. Further investigation reveals that the historical recruitment data used to train the model is biased, reflecting past hiring patterns that disadvantaged rural applicants.

When you report the issue to senior management, they acknowledge the problem but insist that retraining the model would delay deployment and increase development costs. They instruct the team to continue with release preparations and "fix the bias later," after the product is launched.

You now face an ethical, professional, and legal dilemma regarding how to respond.

i. What should you do in response to management's instruction to proceed despite the known AI bias? (05 Marks)

ii. Discuss the ethical implications of deploying a biased AI recruitment system and explain the professional responsibilities of IT professionals in such situations. (05 Marks)

iii. Discuss the legal implications of deploying a biased AI system, including potential violations of anti-discrimination laws, data-protection requirements, or fairness-related regulations. (05 Marks)

iv. Recommend practical steps that TalentPlus Innovations can take to identify, reduce, or eliminate bias in the AI model before deployment. (05 Marks)

Question 9:

QUESTION ELEVEN (20 MARKS)

Case Study: Data Protection Concerns at SafeRide Transport Services

SafeRide Transport Services is a growing ride-hailing company that manages thousands of customer profiles, driver accounts, and mobile-payment records. During a cybersecurity assessment, you discover that SafeRide stores driver and customer passwords in plain text within its internal database. This exposes users to identity theft, account hijacking, and financial fraud if the database were ever breached.

When you escalate the issue to senior management, they downplay the risk, claiming that implementing password hashing, encryption, and modern authentication controls would be too expensive and slow down development. They advise you to ignore the issue and complete your consultancy report without mentioning it.

You now face a professional, ethical, and legal dilemma regarding whether to report the issue, escalate internally, or take other action.

i. Should you report SafeRide's insecure password-storage practices to a regulatory authority, even if it risks your job or consulting contract? (05 Marks)

ii. Discuss the ethical considerations involved, including professional responsibility, whistleblowing, duty of care, and potential harm to users. (05 Marks)

iii. Discuss the legal considerations, including data-protection laws, liability risks, regulatory requirements, and your obligations as a cybersecurity professional. (05 Marks)

iv. Recommend practical steps that SafeRide should take to securely store user passwords and strengthen its overall data-protection posture. (05 Marks)

Question 10:

QUESTION TWELVE (20 MARKS)

Case Study: Confidential Design Conflict at BrightApps Solutions

You are a freelance developer working on custom software solutions for multiple clients. BrightApps Solutions hires you to build a predictive maintenance system for its smart-home devices. During the project, you are given access to BrightApps' proprietary machine-learning model, which uses a unique feature-engineering process and optimisation algorithm that significantly improves prediction accuracy.

Shortly after, another client—HomeSense Technologies, a direct competitor in the smart-home market—offers you a more lucrative contract on the condition that you incorporate similar optimisation techniques into their system. They insist that you "use your experience" from other projects, without explicitly asking for code transfer. You now face an ethical and legal dilemma regarding intellectual property, confidentiality, and conflict of interest.

i. How should you handle this situation while respecting professional and ethical obligations? (05 Marks)

ii. Describe the potential ethical issues that arise when working with competing clients in the same industry. (05 Marks)

iii. Describe the potential legal issues that may arise when working with competing clients, especially regarding confidentiality and intellectual property. (05 Marks)

iv. Recommend practical strategies freelancers can implement to avoid conflicts of interest and protect client intellectual property when handling multiple projects. (05 Marks)

Question 11:

QUESTION THIRTEEN (20 MARKS)

You are a data scientist working on a large-scale clinical trial evaluating the safety and effectiveness of a new pharmaceutical drug. Preliminary statistical analyses indicate no significant improvement over existing standard treatments. When you share these findings, your supervisor privately suggests that you 'adjust the model', selectively remove outliers, and revise the reporting format so that the drug appears more effective. He argues that presenting 'positive results' will increase the likelihood of regulatory approval, attract

investors, and justify continued research funding. You must decide how to respond to this request while maintaining scientific integrity.

i. Discuss the implications of manipulating scientific data in terms of ethical and professional responsibility. (05 Marks)

ii. Discuss the legal implications of manipulating scientific data in a regulated industry such as healthcare or pharmaceuticals. (05 Marks)

iii. Explain the potential consequences of falsified clinical data on patient safety, public trust, and long-term scientific progress. (05 Marks)

iv. If you were the data scientist in this scenario, describe the steps you would take to address the supervisor's request while upholding research integrity and protecting yourself professionally. (05 Marks)

Question 12:

QUESTION FOURTEEN (20 MARKS)

A popular tech blogger publishes a widely circulated online review alleging that a newly released smartphone model from a major technology company contains a serious security flaw that exposes users to significant cybersecurity risks. The company asserts that the allegation is false, misleading, and damaging to its brand reputation, consumer trust, and ongoing sales. They are considering legal action for digital defamation but must evaluate the legal, evidential, and practical dimensions of such a case.

i. Evaluate the legal grounds for a defamation claim and explain the type of evidence the company would need to present. (05 Marks)

ii. Discuss the potential defenses the blogger could raise to counter the company's defamation claim. (05 Marks)

iii. Analyze the major challenges the company might face in pursuing a digital defamation lawsuit, especially in cross-border or online contexts. (05 Marks)

iv. If you were advising the company, outline non-litigation strategies (e.g., public relations, technical audits, negotiations) that could be used to address the situation ethically and effectively. (05 Marks)