1. A software engineer at a tech company discovers a critical vulnerability in a widely used software product. If exploited, it could compromise user data across various industries. Reporting the issue would require disclosing it publicly, potentially alarming users and competitors. However, withholding it until a solution is developed may lead to exploitation if the vulnerability is discovered by malicious actors.
a. List the possible courses of action the engineer could take and analyze each according to professional ethics.
b. Which clauses of the ACM Code of Conduct would support reporting vs. withholding this information?

1. Vulnerability Disclosure by Software Engineer

a. Possible Courses of Action and Analysis

1. **Report Immediately**: Disclose the vulnerability publicly, ensuring transparency.
   - **Pros**: Prevents malicious exploitation if disclosed to relevant parties.
   - **Cons**: Might cause panic among users and competitors, impacting reputation.
2. **Report Privately**: Notify the software company or relevant organizations first.
   - **Pros**: Allows the issue to be fixed discreetly, reducing potential harm.
   - **Cons**: Risk of malicious discovery before a solution is implemented.
3. **Withhold Information**: Delay reporting until a solution is developed.
   - **Pros**: Prevents public panic.
   - **Cons**: High risk of exploitation by malicious actors during the delay.

b. ACM Code of Conduct Clauses

- **Supports Reporting**:
  - **1.1 Contribute to Society and Human Well-Being**: Sharing the vulnerability prevents harm to users.
  - **1.3 Be Honest and Trustworthy**: Transparency builds trust in the professional community.
- **Supports Withholding**:
  - **2.2 Avoid Harm**: Ensures harm is mitigated before public disclosure.
  - **3.1 Ensure Proper Management of Systems**: Taking time to fix the issue supports system stability.

2. An IT manager at a healthcare facility discovers that an employee has accessed confidential patient records without authorization. The manager has the authority to report the incident to higher authorities but worries about the potential consequences for the employee’s career.
a. Should the IT manager report the incident, or handle it privately? Explain using the ACM Code of Conduct.
b. What are the potential legal implications of failing to report the unauthorized access?

2. Unauthorized Access to Patient Records

a. Should the IT Manager Report or Handle Privately?
The manager should **report the incident** to higher authorities as per the ACM Code of Conduct:

- **1.2 Avoid Harm**: Failing to report may lead to further unauthorized access, harming patient trust.
- **2.5 Respect Privacy**: Reporting ensures that measures are taken to prevent future breaches.

b. Legal Implications of Failing to Report

- **Violations** under privacy laws (e.g., HIPAA in the US, PECA in Pakistan).
- **Penalties**: The healthcare facility may face fines or lawsuits for negligence.

3. In a bank, a newly implemented transaction monitoring system shows signs of technical instability, with data loss occurring sporadically. Shutting down the system to investigate could prevent data loss but disrupt services.
a. Describe the ethical and professional considerations in deciding whether to shut down the system.
b. Identify applicable ACM clauses and how they would support either immediate action or a less disruptive approach

3. Transaction Monitoring System Failure

a. Ethical and Professional Considerations

- **Shut Down Immediately**:
  - Prevents further data loss, prioritizing integrity.
  - Disrupts services, affecting customers.
- **Continue Operations**:
  - Ensures availability but risks further data loss.
- **Balanced Approach**:
  - Reduce operations to critical services while investigating.

b. ACM Clauses Supporting Action

- **Supports Immediate Shutdown**:
  - **1.2 Avoid Harm**: Prevents harm to customers due to data loss.
- **Supports Less Disruptive Action**:

    - **2.9 Design and Maintain Systems for High Reliability**: Ensures continued service while resolving issues.

4. A government agency uses software that monitors employees' online activity to protect against
internal threats. An employee claims that the monitoring invades their privacy rights.
a. Explain the ethical implications of using surveillance in the workplace.
b. How should the agency address this complaint while balancing security needs? Discuss relevant ethical principles.

4. Employee Privacy vs. Workplace Surveillance

a. Ethical Implications of Surveillance

- Protects against insider threats but compromises employee privacy.
- Ethical concerns include lack of transparency and potential misuse of data.

b. Balancing Security and Privacy

- Implement clear policies and consent mechanisms.
- Follow **ACM Code of Conduct**:
    - **1.6 Respect Privacy**: Limit surveillance to necessary activities.
    - **3.1 Manage Systems Responsibly**: Protect employee rights while securing the workplace.

5. A cybersecurity consultant detects a malware attack on a client's network. Although they manage to contain it, they discover that the malware had access to sensitive data for an extended
period. Reporting this to affected clients could lead to significant reputational damage for the organization.
a. Outline the ethical and legal responsibilities of the consultant.
b. Which clauses in the ACM Code of Conduct would guide the consultant's actions in
this situation?

5. Malware Incident and Data Exposure

a. Ethical and Legal Responsibilities of the Consultant

- **Ethical**: Inform affected clients to mitigate further harm.

- **Legal**: Follow data breach notification laws (e.g., GDPR, PECA).

b. ACM Clauses

- **1.2 Avoid Harm**: Transparency prevents further damage.
- **2.3 Be Honest About Limitations**: Acknowledge the breach and take responsibility.

6. A data analyst at an e-commerce company finds that a recent data breach exposed customers'
financial data. Management urges the analyst to keep this information confidential until they can mitigate the impact. However, delaying could put customers at financial risk.
a. Discuss the ethical dilemma faced by the analyst, referencing professional codes.
b. What are the potential legal obligations for notifying customers promptly?

6. E-Commerce Data Breach

a. Ethical Dilemma

- **Delay Reporting**: Prevents panic but risks harm to customers.
- **Immediate Reporting**: Ensures customer protection but might affect reputation.
- **ACM Guidance**:
  - **1.2 Avoid Harm**: Prioritize customer safety.
  - **2.5 Respect Privacy**: Ensure customers are informed.

b. Legal Obligations

- Many jurisdictions require prompt notification under laws like GDPR or PECA.

7. A newly hired information security analyst at a financial institution discovers a significant vulnerability during routine security audits. It could potentially lead to unauthorized access to sensitive customer data, financial records, and intellectual property. S/he understands that by exploiting this vulnerability anyone could gain unauthorized privileges and access confidential information within the organization's systems. However, such actions would directly violate

your professional code of ethics and the trust placed on you by the employer. Thus, s/he faces a significant ethical dilemma and must choose between:
i. Reporting the Vulnerability: Acting by your professional obligations and ethical principles, you immediately report the vulnerability to your supervisor or the appropriate security team within the organization. By doing so, you ensure that the issue is addressed promptly and responsibly, mitigating potential risks.

ii. Unauthorized Access: Opting to exploit the vulnerability to gain access to the system, solely to verify its severity and gather concrete evidence. This evidence would be crucial when reporting the vulnerability to the appropriate channels.
Express your answer as per the coverage and style we discussed in class.

7. Significant Vulnerability in Financial Institution

a. Ethical Dilemma

1. **Reporting the Vulnerability**:
    - Ethical and responsible action.
    - Avoids violating trust and professional standards.
2. **Exploiting the Vulnerability**:
    - Violates **2.3 Be Honest** and **1.2 Avoid Harm** of ACM Code.
    - Could harm the organization and undermine the analyst’s reputation.

Recommendation: Reporting ensures ethical compliance and mitigates risks.

8. Select the two most applicable clauses from the PECA 2016 act, which apply to the hackers in
the following scenarios:
i. Aliya, a successful entrepreneur, finds herself a victim of identity theft. The hackers have obtained her personal information through social engineering tactics. With this information, they gain unauthorized access to her online banking and credit card accounts, conducting fraudulent transactions in her name. Aliya's financial stability and reputation are at stake.
ii. Farhan, a software engineer, becomes the target of a cyberstalking campaign. The hackers, driven by personal hatred, use Farhan's personal information to harass him relentlessly online. They send him malicious and threatening messages, post defamatory content on social media platforms, and attempt to tarnish his professional reputation. Farhan's mental well-being and professional growth are severely impacted.

8. PECA 2016 Application

i. Identity Theft (Aliya)

- **Clause 16**: Unauthorized use of identity information.
- **Clause 13**: Electronic fraud by causing harm through data manipulation.

ii. Cyberstalking (Farhan)

- **Clause 24**: Cyberstalking through online harassment.
- **Clause 20**: Harm to reputation via false information.

PECA 2016 Act Application:
9. Choose the most relevant PECA 2016 clauses that apply to the following scenarios:
i) A hacker breaches a company's database, accessing and selling customer data without permission.
ii) A disgruntled employee is caught manipulating data in a financial institution's systems to harm the company's operations.

(Answer using specific clauses from PECA 2016 covered in the readings and slides.)

9. PECA 2016 Scenarios

i. Data Breach

- **Clause 5**: Unauthorized access to information systems.
- **Clause 13**: Theft and sale of customer data.

ii. Data Manipulation

- **Clause 15**: Malicious use of systems to harm operations.
- **Clause 7**: Unauthorized interference with critical infrastructure.

10. Give short but accurate explanations:
i. How do Non-disclosure Agreements (NDA) between an Employer and Employees facilitate information security?
ii. Why security of digital artefacts created by the employees important for the organization?
iii. Why is Cybercrime hard to prosecute? Explain using an IT scenario.
iv. Compare Law with Ethics on four points in tabular format.
v. List TWO distinct areas each of Information Security, Cyber Security, and Network Security

10. Short Explanations

i. NDAs and Information Security

- NDAs protect sensitive company information by legally binding employees to confidentiality.

ii. Security of Digital Artifacts

- Prevents misuse or theft of intellectual property, protecting the organization's competitive edge.

iii. Difficulty in Prosecuting

Cybercrime

- Global nature, anonymity, and lack of jurisdiction make cybercrime hard to track.
- **Example**: A hacker in one country targeting servers in another.

iv. Comparison of Law vs. Ethics

Law	**Ethics**
Enforced by authorities	Self-regulated by society
Defined by statutes	Based on moral principles
Punishable violations	No legal punishment
Clear rules and penalties	Often subjective

v. Areas of Information Security, Cybersecurity, and Network Security

- **Information Security**: Data protection, Access controls.
- **Cybersecurity**: Malware protection, Incident response.
- **Network Security**: Firewall configuration, Intrusion detection

Legal Scenarios:
1. Leo Snow is a skilled cybersecurity expert with deeply rooted hatred towards a political figure. Determined to create confusion, he coordinates a disinformation campaign. He starts by gaining unauthorized access to a critical infrastructure information system by breaching the security protocols of a government database containing secret information. He then

manipulates authentic documents related to national security, injecting small but misleading details to frame the political figure for spying. In addition, he releases deepfake videos on various online platforms to show the political figure's involvement in unethical and criminal activities. He also employs spamming techniques to disseminate manipulated content across

social media channels, resulting in the rapid spread of false information and causing widespread panic and public outcry.
Answer the following question for the scenario:
i. Identify FOUR legal issues as stated in the Prevention of Electronic Crime Act 2016.
[2]
ii. Name victims entities (other than Leo and the political figure) because of various security violations.
iii. Identify TWO key law enforcement challenges in this scenario. Write 3-4 lines detailing each.

Legal Scenarios

i. Legal Issues in the Case

1. **Unauthorized access** (Clause 5).
2. **Data manipulation** (Clause 13).
3. **Disinformation** (Clause 9).
4. **Spamming** (Clause 25).

ii. Victim Entities

- Government agencies, Public citizens, Media platforms.

iii. Law Enforcement Challenges

1. **Cross-border complexity**: Requires international cooperation.
2. **Sophistication of techniques**: Identifying the attacker and countering deepfake technologies

List the clauses of Pakistan law called Prevention of Electronic Crime Act, 2016 that provides legal action against cybercrimes you described in part (a) above.
Correct answer must list three crimes will give one line description and 2-3 line scenarios.
Hate speech
Electronic forgery and electronic fraud
Identity theft
Dignity/Modesty of a natural person.
Promoting malicious code

Cyber Stalking
Spamming
Copyright violation
Piracy (Software)

b. List two different ethical issues in information security. Suppose an IT manager has access to video footages of all cameras across some corporate campus. Explain ONE ethical responsibility, as per the corporate ethical code of conduct that the IT manager must follow while accessing these video.

Two key issues are: i) compromising individual or corporate privacy and ii) Personal integrity and honesty.

The two issues listed above are key responsibility of IT manager while being the custodian of the videos. The student need to write some key step of code of conduct that the IT manager will use while accessing videos and keeping secondary information (the non-relevant information he/she gained by look at relevant parts of the videos) must be kept confidential all the times.