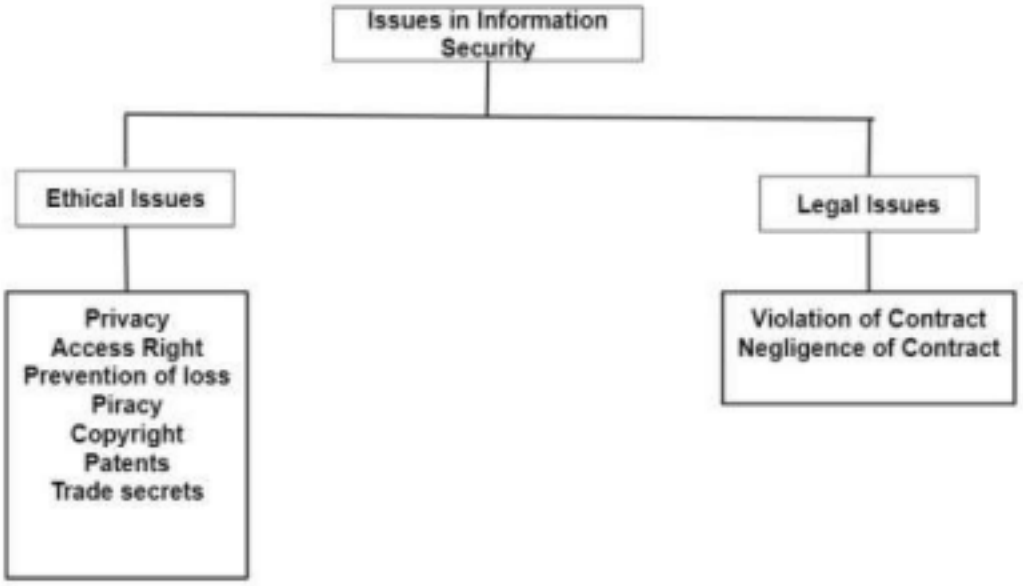
Worksheet: Report writing on legal issues and ethics with respect to some case study.

1. Understand ethical and legal issues in information security



2. Read : https://www.bartleby.com/subject/engineering/computer science/concepts/ethical-and-legal-issues#common-mistakes

Work to be done:

1. Choose a coding project. Refer example cases#and state the hypothetical scenario in detail. Imagine that you are asked to develop the solution. With respect to the expected project work, Study various ethical and legal scenarios and decide on a course of action.
2. Refer the ACM case studies and their analysis of the situations describing violations of code of ethics
3. To evaluate the ethics of each situation, you can use the following ethical decision making model:
    a. Describe the ethical dilemma;
    b. Identify the stakeholders;
    c. Outline your options and how each group of stakeholders will be affected;
    d. Make a decision among the options you've identified.

    3. After you've developed a strategy/made a decision, examine the ACM Code of Ethics for the chosen problem. Check if your action(s) align with the Code? Why or why not? Justify your answer.
    4. How could you fix the scenario to follow all legal and ethical compliance?

References:

2. GENERAL ETHICAL PRINCIPLES. https://www.acm.org/code-of-ethics#h-1.-general ethical-principles.

3. **ACM code of ethics:** https://www.acm.org/code-of-ethics
4. Ethical Coding: Privacy, Ethics & Law in Computing

https://files.eric.ed.gov/fulltext/EJ1258145.pdf

5. # Some case studies https://www.pmi.org/-/media/pmi/documents/public/pdf/ethics/ethics-complaints/sample-ethics cases.pdf?v=6122162d-e8ff-431f-9c63-9dbc9351b1d7
6. # Example problems:
    a. You are asked by your employer, a pharmaceutical company, to design a website to promote a drug they have developed. The law prohibits direct medical marketing to consumers at this time, so the company asks you to design the general information site as an online quiz, where users do not know it relates to the drug company. The target audience is teenaged girls. When taking the quiz, participant answers may vary, but the site always recommends the same drug (your company's target product). Sometimes the drug may be harmful to the user, depending on how they answer the quiz.
    b. You are asked by your employer, a company that builds and programs self driving cars, to design the "object avoidance" feature of the vehicles. You currently need to determine what the car will collide with when sandwiched between a stationary object (which could injure/kill the vehicle occupants) and a human moving target, such as a bicyclist or motorcyclist. All you know is that there is the potential for someone to be injured or killed by the programming, and the car needs to hit one of the two targets.
    c. You are asked by your employer, a major clothing brand retailer that focuses on one gender, to program a competition on their website for entrants to win prizes, such as an iPhone. The company also asks you to write code to extract five random winners. Management, however, only wants winners to come from the targeted gender.
7. #https://www.acm.org/code-of-ethics/case-studies
8. https://pressbooks.pub/bus206/chapter/chapter-12-the-ethical-and-legal-implications-of information-systems/

Name: Vedansh Savla
Roll No.: 16010122323
Div: C-1
Date: 23/04/25
Subject: Information Security Lab

Exp No.: 10

Case Study 1

An organization is in the process of developing an internal employee management system designed to store and manage various types of sensitive employee information, including identification numbers, salary data, performance reviews, and medical records. As part of the development team, you're tasked with ensuring that the system is secure and compliant with data privacy laws such as the GDPR and CCPA, while also adhering to internal policies. However, during the course of development, some challenges arise. In an effort to improve system performance, certain team members propose storing sensitive data in an unencrypted format, arguing that it would speed up database operations and improve overall efficiency. Additionally, there are internal suggestions from management and some developers to implement administrative backdoors in the system. These backdoors would allow select users to bypass regular security measures and gain unrestricted access to all employee records, under the justification that it would simplify administrative tasks and reduce the time needed for access management. This proposal raises significant ethical and legal concerns, as implementing such features would directly compromise employee privacy and create substantial vulnerabilities, increasing the risk of data breaches or unauthorized access. As a developer and ethical professional, you are now faced with a dilemma: whether to comply with the organization’s requests to introduce insecure and non-compliant elements into the system for the sake of convenience, or to oppose these decisions in favor of building a secure, privacy-respecting solution that aligns with both legal requirements and professional ethical standards.

1. Hypothetical Scenario - Coding Project

For this task, imagine a scenario where you are asked to develop a solution for an organization that is seeking to implement an internal employee management system. The system will store personal and sensitive data such as employee identification numbers, salaries, performance reviews, medical information, and other confidential data. You are tasked with ensuring the system is secure and compliant with applicable privacy laws and organizational policies.

During the course of development, it becomes clear that the system may store sensitive data in an unencrypted format to improve performance. Furthermore, some team members suggest creating "backdoors" in the system to allow administrators easy access to all employees’ personal information, bypassing the usual security protocols for ease of use.

The ethical dilemma in this scenario is whether or not to comply with the request to develop backdoors or to ensure that the system is secure, adheres to privacy laws, and upholds ethical standards in information security.

Study of Various Ethical and Legal Scenarios

In this situation, the ethical and legal concerns would involve:

- **Privacy Violations**: Storing unencrypted sensitive data is a clear violation of data privacy laws such as GDPR or CCPA (California Consumer Privacy Act), which mandate that personal data must be stored securely and only accessed by authorized personnel.
- **Backdoor Access**: Developing backdoors in a system intentionally opens up opportunities for data breaches and unauthorized access, which is illegal in most jurisdictions and unethical in the realm of information security.
- **Duty of Care**: As a developer, there is a duty to protect user data from misuse, hacking, and unauthorized access, in line with both ethical codes (such as ACM's Code of Ethics) and legal standards.

2. ACM Case Studies and Analysis of Violations of Code of Ethics

Referring to ACM case studies, one that aligns closely with the current situation involves the breach of trust and integrity in the software development process. The **ACM Code of Ethics** stresses that software professionals must act in the best interest of the public and avoid harm, particularly in situations involving sensitive data (ACM Code of Ethics, 1.2.1 and 1.3.3). The scenario of creating backdoors and unencrypted data violates the following sections of the ACM Code of Ethics:

- **Section 1.2.1**: "Contribute to society and human well-being, acknowledging that all people are stakeholders in computing."
- **Section 1.3.3**: "Ensure that the system is reliable and secure."
- **Section 2.3.3**: "Be honest and trustworthy."

These sections align with the ethical violations in the hypothetical case where sensitive data would be mishandled or vulnerable to unauthorized access.

3. Ethical Decision-Making Model

a. Describe the Ethical Dilemma: The ethical dilemma is whether to follow the team's request to include unencrypted storage of sensitive data and create backdoors for administrative access,

compromising both legal compliance and ethical standards, or to uphold security and privacy, thereby possibly facing resistance from management and other team members.

b. Identify the Stakeholders:

- **Primary Stakeholders**: Employees whose personal data is being stored and managed by the system.
- **Secondary Stakeholders**: The development team and project managers.
- **Tertiary Stakeholders**: The organization and its leadership, who may have a vested interest in maintaining system performance and ease of administration.
- **External Stakeholders**: Regulators or privacy authorities (depending on the legal jurisdiction), whose role is to ensure legal compliance.

c. Outline Your Options and How Each Group of Stakeholders Will Be Affected:

- **Option 1**: Implement the requested backdoors and unencrypted storage for ease of administration.
    - **Effect on stakeholders**:
        - Employees: Their sensitive data could be compromised, violating their privacy rights.
        - Development Team: May face internal pressure but could contribute to a solution that compromises ethics.
        - Organization: Could face legal penalties or loss of trust.
        - Regulators: The organization could be fined for non-compliance with privacy laws.
- **Option 2**: Refuse to create backdoors and ensure that data is encrypted and securely stored.
    - **Effect on stakeholders**:
        - Employees: Their data remains secure and compliant with privacy laws, which builds trust.
        - Development Team: May face pushback, but ultimately contributes to a more secure, ethical solution.
        - Organization: Could face resistance but gains a reputation for compliance and responsibility.

    - Regulators: The organization ensures compliance, avoiding penalties.

d. Make a Decision Among the Options You've Identified: I would choose **Option 2**, where data is encrypted and no backdoors are created. This decision upholds the integrity of the project, ensures compliance with privacy laws, and protects employees' sensitive information.

4. Does the Decision Align with the ACM Code of Ethics?

Yes, **Option 2** aligns with the **ACM Code of Ethics** for the following reasons:

- **Section 1.2.1** (Public Interest): The decision to protect employees' personal data contributes to human well-being and societal interests, ensuring that personal information is handled responsibly and ethically.
- **Section 1.3.3** (Ensure System Reliability and Security): The decision supports the creation of a secure system that is resilient to unauthorized access and data breaches.
- **Section 2.3.3** (Honesty and Trustworthiness): By rejecting the creation of backdoors and unencrypted storage, the decision maintains trustworthiness and transparency.

The ethical choice ensures that the project maintains both legal and ethical compliance, safeguarding the organization's reputation and protecting the privacy of individuals.

5. Fixing the Scenario to Follow Legal and Ethical Compliance

To fix the scenario, I would recommend the following actions:

- **Implement Strong Encryption**: Ensure that all sensitive data, such as employee medical information and salary details, is stored using end-to-end encryption. This guarantees that the data is protected, even if the system is breached.
- **No Backdoors**: Do not allow any backdoors in the system, even for administrators. Access to sensitive data should be logged and monitored, with access limited to authorized personnel only, and governed by strict roles and responsibilities.
- **Compliance Training**: Provide mandatory compliance and ethical training to all team members to reinforce the importance of data security, privacy, and ethical behavior in software development.
- **Regular Audits and Reviews**: Implement periodic audits and security reviews to ensure that the system is compliant with privacy laws and organizational standards.
- **Transparency with Stakeholders**: Maintain open communication with all stakeholders regarding the importance of protecting sensitive data and the steps taken to ensure

security and compliance.

By addressing these actions, the organization can maintain legal and ethical compliance, reduce the risk of data breaches, and protect employees' personal information.

Case Study 2

Joseph desired to use an internet domain address for his project management services business, and the domain name included direct identification of PMI (joetrain.pmi.org). Since he wanted to use the PMI.org domain, Joseph requested the ability to do so from PMI. PMI declined his request since it would lead people to believe that PMI endorsed or otherwise recommended Joseph's training, and the decision was upsetting to Joseph. Joseph contacted PMI and stated that he felt PMI's decision was unfair. He then started texting certain PMI staff members with dozens of texts per day. PMI then sent to Joseph an email advising him that PMI would not change its decision and directed Joseph to stop texting and calling. However, Joseph sent additional texts that were rude and threatened legal action, claiming he had significant influence with the government and others involved in domain name assignment. Joseph continued his messaging at a rate of five dozen messages in less than a half day. In parallel to his communications to PMI headquarters staff, he sent multiple communications with the local Chapter President and threatened PMI and the local Chapter with various actions (like litigation). The Chapter President reached out to Joseph and requested that he stop sending messages – these were not constructively working toward a resolution. When he did not stop, the Chapter President filed a formal ethics complaint, alleging that Joseph had violated the value of respect, specifically section 3.3.3 of the code: Section 3.3.3 (Respect) - We do not act in an abusive manner to others. An ERC Review Team was assigned and performed a detailed investigation of the charges and reviewed the documented communications. After initially stating he was not able to communicate to PMI ERC on the ethics issues due to internet connectivity problems, Joseph then chose not to respond in any way to the ethics charges. Later, Joseph sent a note admitting to the ethics charges and apologizing for his behavior. An Ethics Hearing was held. The ERC Hearing Panel concurred with the charges. They stated that it is contrary to the Code of Ethics and Professional Conduct to act in an abusive manner toward others, including the excessive use of emails, text messages, or other forms of correspondence. Correspondence always should be professional and measured.

1. Hypothetical Scenario - Domain Name Request

Joseph desired to use an internet domain address for his project management services business that included PMI's domain (e.g., **joetrain.pmi.org**). PMI declined his request because it could imply endorsement by PMI. Upset by the decision, Joseph began sending excessive, rude, and threatening messages to PMI staff and the local Chapter President.

The ethical dilemma here is whether Joseph's repeated communications, including threats and harassment, are acceptable forms of conflict resolution, or whether they violate professional ethical standards of respect and professionalism.

Ethical and Legal Issues:

- **Harassment and Threatening Behavior**: Sending excessive, rude, and threatening messages is abusive and violates the ethical standard of respect.
- **Professional Conduct**: Ethical standards for professional communication must be upheld, including respect for others and measured, constructive responses to disagreements.

---

2. ACM Case Studies & Violations of Ethics

Joseph's behavior violates ethical standards similar to those found in **ACM's Code of Ethics**:

- **Section 1.3.2**: "Honor confidentiality" — In this case, sending personal and persistent messages to PMI staff may breach the ethical duty to respect boundaries and professionalism.
- **Section 2.3.3**: "Be honest and trustworthy" — Joseph's abusive communications and threats undermine trust.
- **Section 3.3.3** (Respect): "We do not act in an abusive manner to others" — Joseph's actions clearly violate this section, as he repeatedly sent harassing and disrespectful messages after being asked to stop.

---

3. Ethical Decision-Making Model

a. Ethical Dilemma: Whether Joseph's repeated, abusive communications in response to a declined domain name request are justified or violate ethical conduct standards.

b. Stakeholders:

- **Joseph**: Upset by PMI's decision and seeking resolution.
- **PMI Staff**: Recipients of abusive communication.
- **Chapter President**: Person receiving threats and trying to de-escalate the situation.
- **PMI Organization**: Must protect its reputation and ensure a respectful environment.

c. Options & Effects:

- **Option 1**: Continue sending aggressive messages in an attempt to get a favorable response.
    - **Effects**:
        - Joseph: Potentially damaging his professional reputation.
        - PMI: Could face harassment and possible legal consequences.
        - Chapter President: Forced to handle unwanted, aggressive communication.
- **Option 2**: Stop sending excessive messages and resolve the issue through formal, respectful channels (e.g., legal action or dispute resolution).
    - **Effects**:
        - Joseph: Preserves his professionalism and reputation.
        - PMI: Can handle the issue without further disruption.
        - Chapter President: No further stress or unnecessary confrontation.

d. Decision: Choose **Option 2** to resolve the issue professionally and avoid further damage to Joseph's reputation and PMI's organizational harmony.

---

4. Does the Decision Align with ACM Code of Ethics?

Yes, **Option 2** aligns with the **ACM Code of Ethics**:

- **Section 1.3.2**: Encourages respectful and professional conduct when resolving issues.
- **Section 2.3.3**: Upholding honesty and trustworthiness requires Joseph to acknowledge that continued harassment is inappropriate.

- **Section 3.3.3**: Joseph's decision to cease abusive communications would align with the expectation of acting with respect and professionalism in all dealings.

By following this course of action, Joseph would uphold the ACM Code of Ethics by maintaining professionalism and avoiding abusive behavior.

---

5. Fixing the Scenario for Compliance

To fix the scenario and follow ethical guidelines:

- **Cease Abusive Communication**: Joseph must immediately stop sending excessive, threatening messages and respect PMI's requests.
- **Use Formal Channels**: If Joseph wishes to dispute PMI's decision, he should do so through formal legal channels or professional mediation, not harassment.
- **Apology and Professionalism**: Joseph should issue a formal apology to PMI staff and the Chapter President, acknowledging his mistake and committing to respectful future interactions.
- **Conflict Resolution Training**: Both PMI and Joseph should be encouraged to use constructive methods to resolve conflicts, such as negotiation or third-party mediation.

By adhering to these actions, Joseph can rectify his behavior and align with ethical and professional standards.

Case Study 3

Sam Jones was reading an article by Sally Smith on a popular project management web site. It was on scheduling, a topic he was very interested in, and he did some additional reading. As he researched the information, Sam realized that a lot of information used by Sally was directly copied from another source. Sam wanted to contact Sally, but was unable to find an email address or phone number he could call. He also sent a note to the web site via their contact page, but it went unanswered. Sam re-checked the article and facts, and submitted an ethics complaint via the PMI web site. He felt that Sally had violated the core value of honesty: 5.3.1 (Honesty) -

We do not engage in or condone behaviour that is designed to deceive others, including but not limited to, making misleading or false statements, stating halftruths, providing information out of context or withholding information that, if known, would render our statements as misleading or incomplete. The Ethics Review Committee accepted that there was a case to answer and a Review Team was established. After investigation the Review Team decided that the value of respect was also violated: 3.3.4 (Respect) - We respect the property rights of others. A hearing was scheduled by the ERC. At the hearing Sally admitted that she had in fact copied material from another author and not acknowledged that author. But she also felt there were some mitigating circumstances – the article was not meant to be published as it was and there was some miscommunication between Sally and the web site publisher. Sally said she did not do this deliberately and wished to correct any error. The hearing panel for this case determined that only code section 3.3.4 had been violated. A private reprimand was issued. Important factors in the ERC's consideration of what sanction should apply were the fact that Sally was remorseful, admitted that she had made an error, and sought to correct the error.

1. Hypothetical Scenario - Plagiarism and Ethics Complaint

Sam Jones reads an article on project scheduling by Sally Smith and notices that much of her content appears to be directly copied from another source without proper attribution. Unable to contact Sally directly, Sam submits an ethics complaint to PMI, alleging that Sally violated PMI's code of ethics, particularly regarding honesty and respect for intellectual property.

The ethical dilemma involves whether Sally's actions of copying content without attribution constitute a breach of professional ethics, and whether Sam's complaint is a valid response to address the issue.

Ethical and Legal Issues:

- **Plagiarism**: Copying content without proper attribution is dishonest and violates intellectual property rights.
- **Violation of Respect**: By failing to give credit to the original author, Sally violated respect for intellectual property rights.

---

2. ACM Case Studies & Violations of Ethics

Sally's actions violate ethical standards outlined in **ACM's Code of Ethics**:

- **Section 5.3.1** (Honesty): "We do not engage in or condone behavior that is designed to deceive others." Plagiarism is a clear violation of this section, as it misleads readers into believing that Sally is the original author.
- **Section 3.3.4** (Respect): "We respect the property rights of others." By using someone else's work without permission or attribution, Sally violated the property rights of the original author.

These violations highlight the importance of honesty and respect for intellectual property in the professional and academic environment.

---

3. Ethical Decision-Making Model

a. Ethical Dilemma: Whether Sally's failure to attribute the source of her article is justified, or if it is a violation of ethical standards concerning honesty and respect.

b. Stakeholders:

- **Sally Smith**: The author of the article, who is responsible for the content.
- **Sam Jones**: The individual who identified the issue and filed the ethics complaint.
- **Original Author**: The person whose work was copied without attribution.
- **PMI and the Web Publisher**: They are responsible for ensuring that ethical standards are maintained in published content.

c. Options & Effects:

- **Option 1**: Sally denies the plagiarism or claims it was an accident, avoiding accountability.
    - **Effects**:
        - Sally: Continues to work without acknowledging her mistake, damaging her reputation.
        - Original Author: Their intellectual property remains unrecognized.
        - Sam: His ethics complaint is dismissed, and the issue persists.
- **Option 2**: Sally admits the mistake and seeks to correct the error.

- **Effects**:
  - Sally: Takes responsibility and shows remorse, maintaining her professional integrity.
  - Original Author: Receives credit for their work, restoring their intellectual property rights.
  - Sam: His complaint is validated, and the issue is addressed ethically.

d. Decision: Choose **Option 2** to resolve the issue ethically by admitting the error, correcting it, and giving credit to the original author.

---

4. Does the Decision Align with ACM Code of Ethics?

Yes, **Option 2** aligns with the **ACM Code of Ethics**:

- **Section 5.3.1**: Acknowledging the mistake and correcting the error upholds honesty and ensures no further misleading statements.
- **Section 3.3.4**: Giving proper attribution to the original author aligns with respecting intellectual property rights.

Sally's actions would demonstrate professionalism and ethical responsibility by correcting the error and giving credit to the original source.

---

5. Fixing the Scenario for Compliance

To fix the scenario and ensure compliance with ethical standards:

- **Admit the Mistake**: Sally should publicly admit her mistake and issue a correction that gives credit to the original author.
- **Proper Attribution**: Moving forward, Sally must ensure that all sources are correctly cited in her articles to avoid plagiarism.
- **Apology to the Original Author**: Sally should reach out to the original author and apologize for the oversight and failure to credit them properly.
- **Educational Effort**: Sally could take this opportunity to learn more about intellectual property rights and plagiarism to avoid similar issues in the future.

By taking these steps, Sally can align her actions with the ACM Code of Ethics and restore her credibility as a professional in the field.