---------- Part I ----------

[CLO # 2 – Legal and Ethical Issues in Information Security]

Question 1: [10]
Time: 40 Minutes.

a) Ethical Scenario:

As an information security officer at a government agency, you hand sensitive information critical to national security. The agency has recently implemented a new information system to enhance efficiency in processing and storing classified data. As part of your responsibilities, you discover a potential vulnerability in the system that could be exploited by external actors, posing a significant threat to the confidentiality and integrity of the classified information. However, disclosing this vulnerability to the system developers and initiating the necessary updates would require temporarily shutting down the system. This shutdown, even if brief, could disrupt ongoing intelligence operations and potentially compromise vital national security initiatives. On the other hand, failing to address the vulnerability could lead to unauthorized access and potential leaks of sensitive information. As the information security officer, you face a challenging ethical dilemma:

1. Do you immediately report the vulnerability and advocate for the system shutdown, prioritizing the security of the classified information?
2. Do you withhold information about the vulnerability temporarily, allowing ongoing operations to continue while working with the development team to address the issue without shutting down the system?
3. Do you assess the situation further, considering the potential impact of the vulnerability and the feasibility of addressing it without a system shutdown, before deciding on a course of action?

Answer the following for this scenario based on ACM code of conduct clauses:

i. State ACM clauses that support your decision 1) if you withhold information, 2) report immediately, and 3) take more time for further analysis. Also, explain your selection for each of these decisions. [3]
ii. What you will do when facing this dilemma as the information security officer? [1]

Format answers of both parts as per the below template.

List of clauses related to Q1 a(1)	List of clauses related to Q1 a(2)	List of clauses related to Q1 a(3)
1. 2. 3.	1. 2. 3.	1. 2. 3.
Explanation for withholding information:	Explanation for immediate reporting:	Explanation for further analysis:
Single explanation about what you will do in this situation (5-6 lines).		

b) Legal Scenarios:

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. [2]
iii. Identify TWO key law enforcement challenges in this scenario. Write 3-4 lines detailing each. [2]

[CLO #3 - Analyze/Model/Solve scenario by applying security & risk management tools/techniques]

Question 2: Analyze each of the following brief scenarios and suggest possible solutions along with a detailed explanation of any one solution. Format your answer as per the given template. **[3 x 5=15]**

Time: 1 Hour.

Note:

- *The grader expects you to process each scenario similarly to the format given below.*
- *Solutions falling outside our syllabus will get zero scores.*
- *The same solution specified for different scenarios will be graded once.*

Q2 (a):
Possible solutions: 1. Single-line hint only 2. 3.
Explanation of one solution: (3-4 lines)

a) A series of information security incidents took place in a **recently established** medium-sized company. The management is concerned about the security of information systems including sensitive customer data.

b) Several research institutions are collaborating on a groundbreaking project that involves the exchange and analysis of research data. They need to **exchange data over multiple networks** including the Internet and it contains proprietary algorithms, experimental results, and confidential information critical to the success of the project.

c) The government is modernizing its election infrastructure to conduct secure and tamper-proof elections by a robust mechanism to **validate each voter** during electronic online voting.

d) A pharmaceutical research lab is equipped with state-of-the-art equipment, highly sensitive data, and proprietary research findings. The management wants **real-time security** to safeguard intellectual property and prevent unauthorized access.

e) A manufacturing plant producing electronics relies on an interconnected network to control automated manufacturing processes, monitor equipment, and manage sensitive intellectual property. Recent incidents of **unauthorized access to various servers and bandwidth consumption by outward traffic** raise concerns about potential cyber threats.

----------(O)----------