PENINSULA COLLEGE GEORGETOWN DK266-03(P)

FINAL EXAMINATION

Semester	:	**SEPTEMBER 2025 SEMESTER**
Programme Name	:	**DIPLOMA IN COMPUTER SCIENCE**
Course Code & Name	:	**DCS2243 SECURITY MANAGEMENT**
Duration	:	**3 HOURS**

INSTRUCTIONS TO CANDIDATES:

1. Please read the instructions given in the question paper **CAREFULLY.**
2. The question paper consists of **FOUR (4)** questions.
3. Answer **ALL** questions in the question paper.
4. Answers to the questions are to be written into the examination booklet.
5. Electronic dictionaries, lecture notes, files or any unauthorised materials except writing equipment are strictly prohibited.

This question paper must be submitted along with all used and/or unused rough papers and/ or graph papers (if any). Candidates are **NOT ALLOWED** to take any examination paper(s) used or unused out of the examination hall.

WARNING:

The Examination Board of Peninsula College Georgetown regards cheating as a very serious offence and will not hesitate to mete out the appropriate punitive actions according to the severity of the offence committed, and in accordance with the clauses stipulated in the Students' Handbook, up to and including expulsion from Peninsula College Georgetown.

(*This booklet contains 4 printed pages including this page*)

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE ALLOWED TO DO SO

Answer **ALL** questions on the separate sheet provided. **[100 marks]**

1 **Case Study: Cyberattack on MyMediHealth Clinic**

MyMediHealth Clinic, a private healthcare provider in Kuala Lumpur, recently experienced a ransomware attack that encrypted all patient records and billing data. The attackers demanded RM100,000 in cryptocurrency to unlock the files.
An internal investigation revealed that the clinic's network security had several vulnerabilities — outdated antivirus software, weak passwords used by staff, and no regular data backups.

Following the incident, the management initiated a risk assessment process. The IT team identified critical assets such as patient data, billing systems, and appointment scheduling software. They assessed the likelihood and impact of various threats, ranking ransomware as "high risk."

To prevent future incidents, the clinic implemented several risk control strategies — installing updated firewalls (mitigation), subscribing to cyber insurance (transference), and enforcing multi-factor authentication (avoidance of weak password risks). A Business Continuity Plan (BCP) was also developed to ensure essential services could continue in case of another cyberattack.

a) Analyse the weaknesses in MyMediHealth Clinic's information security system that contributed to the ransomware attack. (6 marks)

b) Based on the risk assessment process, examine how asset identification and vulnerability identification could have helped MyMediHealth Clinic cope with the ransomware attack and reduce its overall impact. (7 marks)

c) Compare and analyze the effectiveness of the three risk control strategies (mitigation, transference, and avoidance) implemented by the clinic. (6 marks)

d) Analyse how continuous monitoring, maintenance, and regular evaluation of security controls could help MyMediHealth Clinic strengthen its cybersecurity posture and prevent future attacks. (6 marks)

Total: [25 marks]

2. **Case Study: Security Policy at MyFinance Bank**

MyFinance Bank in Kuala Lumpur recently faced a problem when some staff used personal USB drives to copy customer data. This created a risk of data leaks and violated company rules.

An internal audit found that the bank did not have clear policies to guide staff on data handling, password use, and system access.

The management then decided to create new information security policies, including:

- Limiting the use of personal devices.
- Encrypting sensitive data.
- Updating antivirus software regularly.
- Conducting staff training on security awareness.

These new policies helped the bank follow Bank Negara Malaysia's guidelines and improve protection of customer information.

a) Explain why MyFinance Bank needs to create clear information security policies for its employees. (6 marks)

b) Describe how the new policies can help protect customer information from data leaks. (6 marks)

c) Discuss how following Bank Negara Malaysia's security guidelines supports MyFinance Bank's information security management. (7 marks)

d) Explain why staff training is important for the successful implementation of information security policies. (6 marks)

Total: [25 marks]

3. **Case Study: MyBank Malaysia and the Data Leak**

In 2023, MyBank Malaysia faced a serious problem when customers' personal data such as names, NRIC numbers, and phone numbers were leaked online. The cause of the leak was a mistake by a third-party company that handled MyBank's customer data.

The Department of Personal Data Protection (JPDP) investigated and found that MyBank failed to ensure the third-party company had strong security controls. This action violated the Personal Data Protection Act (PDPA) 2010, which requires all organizations that collect and process personal data to keep it safe and secure.

The case also showed that MyBank did not show due care and due diligence in protecting customer data. It raised questions about the bank's ethical responsibility to protect personal information and follow Malaysia's data protection laws.

a) Explain how the PDPA 2010 protects customers' personal data in cases like MyBank's data leak. (5 marks)

b) Describe why MyBank is still responsible even though the data was leaked by another company. (5 marks)

c) Discuss how applying due care and due diligence could have helped MyBank prevent the data leak.

(7 marks)

d) Interpret the ethical issues involved in the MyBank case in relation to information security practices. (8 marks)

Total: [25 marks]

4. **Case Study: Cyberattack on Bank Negara Malaysia**

In 2024, Bank Negara Malaysia (BNM) faced a serious cyberattack that caused its online banking systems to go offline for two days. The attack was caused by ransomware that locked several servers containing financial transaction data.

The Incident Response (IR) team quickly tried to stop the attack, but there was confusion because team roles were not clearly defined. Later, it was discovered that the backup systems were not fully updated, causing the loss of six hours of data.

The Disaster Recovery (DR) team worked to restore the systems, while the Business Continuity (BC) team helped banks continue basic services like ATM withdrawals and money transfers.

After the event, a review found three main problems:

- The Incident Response Plan (IRP) did not clearly state who should communicate what.
- The Disaster Recovery Plan was not tested often enough.
- The Business Impact Analysis (BIA) gave the wrong recovery time target (RTO).

BNM decided to improve its Contingency Planning (CP) to make sure all its plans — IR, DR, and BC — work together effectively in future incidents.

a) Analyse how the weaknesses in the Incident Response Plan affected BNM's ability to handle the cyberattack. (6 marks)

b) Examine how problems in the Incident Response Plan, Disaster Recovery Plan, and Business Continuity Plan were connected in this case. (6 marks)

c) Break down the reasons why data was lost even though backups existed. (6 marks)

d) Evaluate how BNM could improve its Contingency Planning process using the NIST 7-step framework. (7 marks)

Total: [25 marks]

- END OF QUESTIONS -