PENINSULA COLLEGE GEORGETOWN

FINAL SEMESTER EXAMINATION

Programme	:	**DIPLOMA IN COMPUTER SCIENCE**
Course	:	**COMPUTER SECURITY AND FORENSIC**
Course Code	:	**DCS2123**
Duration	:	**3 hours**

INSTRUCTIONS TO CANDIDATES:

1. Please read the instructions given in the question paper **CAREFULLY.**
2. This 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.

WARNING:

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

(*This booklet contains 3 printed pages including this page*)

For examiner's use only

QUESTION NO.	MARKS
1	/ 25
2	/ 25
3	/ 25
4	/ 25
Total	**/ 100**

Answer ALL FOUR (4) questions in the separate sheet provided.

Question 1

a. In general, there are **THREE (3)** types of identity authentication tasks. List these tasks. (6 marks)

b. When shopping at Desco, after you've selected your purchases you take your cart full of goods to one of the registers. The check-out clerk scans your goods, totals what you owe, and upon receiving payment from you gives you an itemized receipt. However, you can't then simply exit the building with your goods. At the exit you're required to go by a staff member who inspects your receipt. If the receipt looks okay (appears to match the number and types of items in your cart), the staff member draws a line with a permanent marker down the receipt and hands it back to you. At this point, you can exit the building and take the goods to your car.

i. Identify **TWO (2)** security principles illustrated by Desco's approach. For each, describe in a single sentence what aspect of Desco's approach reflects the principle. (8 marks)

ii. Identify an attack that Desco seeks to prevent by having the staff member draw the line down your receipt. Briefly describe how the attack works. (6 marks)

c. In which situations and for which purposes can cryptography be used to protect information? (5 marks)

Question 2

a. "A trusted system or component is one that can break your security policy". Explain the meaning of this proposition. (4 marks)

b. Briefly explain the following concepts related to identity management. (8 marks)
(i) Entity
(ii) Identity
(iii) Name (identifier)
(iv) Digital identity

c. Briefly explain the concept of "identity management". (3 marks)

d. List the **TEN (10)** goals an ideal password authentication scheme should achieve. (10 marks)

Question 3

a. What are the **SEVEN (7)** goals of incident response? (7 marks)

b. List the **SIX (6)** groups within an organization that may be involved in an incident response. Explain why it is important to communicate with those groups before an incident occurs. (18 marks)

Question 4

a. Explain in detail the **NINE (9)** basic steps of the forensic investigation process. (18 marks)

b. Threats to an organization's cybersecurity are on the rise, but most businesses don't understand how to remediate those threats. Creating a system to identify and fix gaps in your IT systems is essential to a successful cyber risk management program. This process of identifying and fixing problems is called cybersecurity remediation. (7 marks)

Discuss in details when does the remediation process start, and why?

- END OF QUESTIONS -