FINAL
ALTERNATIVE ASSESSMENT

(COVER PAGE)

Session	:	**April 2022**
Programme	:	Diploma in Computer Science (DCS)
Course	:	**DCS2110: Cybersecurity Fundamentals**
Date of Examination	:	August 3, 2022 (Wednesday)
Time	:	4:00 pm – 6:30 pm Reading Time : Nil
Duration	:	2 Hours 30 Minutes

Special Instructions :

Instructions: This paper consists of **FOUR (4)** questions. Answer all **FOUR (4)** questions. All questions carry equal marks.

NOTE : 30 minutes is added into the duration of the examination to factor in any connectivity matters and for you to scan and upload your scripts.

Material permitted :
Nil

Materials provided :
Nil

Examiner(s)	:	**Mr Andrew Ho Mun Wah** and Ms Norashida Sabari
Chief Moderator	:	Mr Vasuky Mohanan

*This paper consists of **4** printed pages, including the cover page*

DIPLOMA IN COMPUTER SCIENCE PROGRAMME (DCS)
DCS2110: CYBERSECURITY FUNDAMENTALS
FINAL ALTERNATIVE ASSESSMENT : APRIL 2022 SESSION

Instructions: This paper consists of **FOUR (4)** questions. Answer all **FOUR (4)** questions. All questions carry equal marks.

Question 1

(a) Although every Cybersecurity framework is different, certain best practices are applicable across the board.

(i) List the **FIVE (5)** best practices of a Cybersecurity framework.

(5 marks)

(ii) Explain with **TWO (2)** appropriate reasoning a suitable Cybersecurity framework that INTI Colleges and Universities Information Technology services and management department should practice for better Information Security Management.

(3 marks)

(b) List and describe **THREE (3)** examples of remote networking attacks that may result in Denial-of-Services.

(6 marks)

(c) Realizing the risks of internal human threats, most company practices some form of surveillance of its employee's computer work devices.

(i) Name **THREE (3)** security software technology that are commonly used for surveillance of employee's computer work devices.

(3 marks)

(ii) Discuss **FOUR (4)** security purposes of surveillance for a business firm.

(8 marks)

(*Total: 25 marks*)

Question 2

(a) List and explain **FOUR (4)** types of cybersecurity risk management strategies**.**

(10 marks)

(b) It is common that application hosts interactive advertisements as a way to generate revenue. However, there are threats of hosting such content that in turn could be a possible malicious adware.

(i) Explain **FOUR (4)** security threats scenarios that may originate from a malicious adware.

(8 marks)

(ii) Identify and describe **TWO (2)** ways to safeguard against malicious adware.

(4 marks)

(c) Differentiate the aim of overt from covert ethical hacking.

(3 marks)

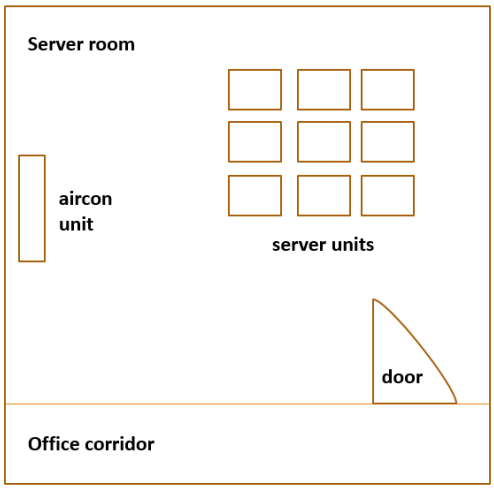
(*Total: 25 marks*)

Question 3

(a) With the aid of a diagram, draw and name the **FIVE (5)** stages of penetration testing.

(5 marks)

(b)



Redraw the above current physical setup of the server room by labeling and explaining **THREE (3)** additional physical security considerations that are most essential.

(6 marks)

(c) Jenny, a security and networking administrator wishes to harden the multi-user Operating System used in the company. Identify and explain **FOUR (4)** techniques she can practice to secure the multi-user Operating System to eradicate vulnerabilities.

(10 marks)

(d) Your college Wi-Fi facility has become an important amenity for students' learning and staffs working purposes. Explain how encryption and authentication provide a logical control environment to secure your college Wi-Fi facility.

(4 marks)

(*Total: 25 marks*)

Question 4

(a) Suggest **FIVE (5)** authentication technologies for logging-in users to a web server that are password-less.

(5 marks)

(b) Social engineering attack techniques are extremely effective in obtaining access to unauthorized information from the employees' working in a business organization.

(i) List **TWO (2)** intangible asset information of the company that are sensitive and confidential which may be gathered from social engineering attack techniques.

(2 marks)

(ii) Explain **TWO (2)** human behaviors that are vulnerable to social engineering attack techniques.

(4 marks)

(iii) As the Cybersecurity Manager in your company, recommend and explain **THREE (3)** countermeasures that can be introduced to employees so that they can be more vigilant against social engineering attack techniques.

(6 marks)

(c) With the use of a table of comparison, compare **TWO (2)** differences between symmetrical encryption standard with asymmetrical encryption standard. For each encryption standard, name **TWO (2)** examples.

(8 marks)

(*Total: 25 marks*)

-THE END-

(DCS2110 (F)/Apr2022/formatted