KEMENTERIAN PENDIDIKAN TINGGI
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI II : 2025/2026

DFC20313 : CYBERSECURITY FUNDAMENTALS

TARIKH : 08 MEI 2026
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

. Kertas soalan ini mengandungi **DUA PULUH DUA (22)** halaman bercetak.
Bahagian A: Objektif (30 soalan)
Bahagian B: Struktur (2 soalan)
Dokumen sokongan yang disertakan : Tiada

JANGAN BUKA KERTAS SOALAN INI SEHINGGA DIARAHKAN

(CLO yang tertera hanya sebagai rujukan)

TERBUKA

SECTION B: 55 MARKS

BAHAGIAN B:55 MARKAH

INSTRUCTION:

This section consists of **TWO (2)** structured questions. Answer **ALL** questions.

ARAHAN:

*Bahagian ini mengandungi **DUA (2)** soalan berstruktur. Jawab **SEMUA** soalan.*

QUESTION 1

SOALAN 1

CLO1 (a) i. Define Information Security

Definisikan Keselamatan Maklumat

[2 marks]

[*2 markah*]

CLO1 (b) i. Compare **TWO (2)** differences between confidentiality and integrity.

*Bandingkan **DUA (2)** perbezaan antara kerahsiaan dan integriti*

[4 marks]

[*4 markah*]

CLO1 ii. Explain **TWO (2)** types of hackers

*Jelaskan **DUA (2)** jenis penggodam*

[2 marks]

[*2 markah*]

CLO1

iii. Explain **FOUR (4)** sources of security threats
*Jelaskan **EMPAT (4)** sumber ancaman keselamatan*

[4 marks]
[4 markah]

(c) i. List **FOUR (4)** types of security attacks.
*Senaraikan **EMPAT (4)** jenis serangan keselamatan*

[4 marks]
[4 markah]

CLO1

ii. Explain **THREE (3)** types of social engineering.
*Jelaskan **TIGA (3)** jenis kejuruteraan sosial.*

[3 marks]
[3 markah]

CLO1

iii. Explain **SIX (6)** step involve in cyber kill methodology phase.
*Jelaskan **ENAM (6)** langkah yang terlibat dalam rantaian pembunuhan siber .*

[6 marks]
[6 markah]

QUESTION 2

SOALAN 2

CLO1 (a) i. List **FOUR (4)** types of security hardening in applications.

*Senaraikan **EMPAT (4)** jenis pengukuhan keselamatan dalam aplikasi.*

[4 marks]

[4 markah]

CLO1 ii. Explain **FIVE (5)** malicious software protection programs.

*Jelaskan **LIMA (5)** program perlindungan perisian jahat*

[5 marks]

[5 markah]

CLO1 iii. Explain **FOUR (4)** physical equipment protection method.

*Senaraikan **EMPAT (4)** kaedah perlindungan peralatan fizikal*

[4 marks]

[4 markah]

CLO1 (b) i. Explain **FIVE (5)** guidelines for creating strong passwords.

*Jelaskan **LIMA (5)** tatacara mewujudkan kata laluan yang kukuh.*

[5 marks]

[5 markah]

ii. In a situation where an organization wants to protect sensitive customer data, apply methods such as data encryption, security tokens, biometrics, and multi-factor authentication to enhance information security.

Dalam situasi dimana organisasi ingin melindungi data sensitif pelanggan, gunakkan kaedah seperti penyulitan data, token keselamatan, biometrik dan pengesahan berbilang faktor untuk meningkatkan keselamatan maklumat.

[4 marks]
[4 markah]

iii. In a system that uses Single Sign-On (SSO), demonstrate **TWO (2)** privilege management to ensure users only access authorized resources

*Dalam sistem yang menggunakan Single Sign-On (SSO), tunjukkan **DUA (2)** pengurusan keistimewaan (privilege management) untuk memastikan pengguna hanya mendapat akses kepada sumber yang dibenarkan*

[4 marks]
[4 markah]

CLO1 (c) i. List **TWO (2)** pillars of information assurances.

*Senaraikan **DUA (2)** tunjang jaminan maklumat.*

[2 marks]
[2 markah]

CLO1

ii. Explain **TWO (2)** pillars of information assurances based on Question 2(c) i.

*Jelaskan **DUA (2)** tunjang jaminan maklumat berdasarkan soalan 2(c)i.*

[2 marks]

[2 markah]

SOALAN TAMAT