SULIT

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 DAN KOMUNIKASI

PEPERIKSAAN AKHIR

SESI I : 2024/2025

DFC20313 : CYBERSECURITY FUNDAMENTALS

TARIKH : 12 DISEMBER 2024
MASA : 8.30 PAGI – 10.30 PAGI (2 JAM)

Kertas ini mengandungi **DUA PULUH TIGA (23)** 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)

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) List **FOUR (4)** primary goals of information security.

*Senaraikan **EMPAT (4)** matlamat utama keselamatan maklumat.*

[4 marks]
[*4 markah*]

(a)(ii) Explain the concepts of integrity and availability in the context of information security.

Jelaskan konsep integriti, dan ketersediaan dalam konteks keselamatan maklumat.

[3 marks]
[*3 markah*]

CLO1 (b)(i) List any **THREE (3)** types of hackers.

*Senaraikan **TIGA (3)** jenis penggodam.*

[3marks]
[*3 markah*]

CLO1 (b)(ii) Describe social engineering by giving **TWO (2)** types of impersonation-based social engineering techniques.

*Huraikan kejuruteraan sosial dengan memberikan **DUA (2)** jenis teknik kejuruteraan sosial berasaskan penyamaran.*

[5 marks]
[*5 markah*]

CLO1 (c)(i) List **TWO (2)** malicious software protection programs.
*Senaraikan **DUA (2)** program perlindungan perisian berniat jahat.*

[2 marks]
[*2 markah*]

(c)(ii) Explain the function of antivirus and antimalware. Give **ONE (1)** example each.
*Terangkan fungsi antivirus dan antimalware. Berikan **SATU (1)** contoh setiap satu.*

[4 marks]
[*4 markah*]

(c)(iii) As a Cybersecurity Analyst in SNE Sdn. Bhd., explain the implementation of **TWO (2)** techniques for application hardening in a web application environment for the SNE Sdn. Bhd.

*Sebagai Penganalisis Keselamatan Siber di SNE Sdn. Bhd., jelaskan pelaksanaan **DUA (2)** teknik untuk pengukuhan aplikasi dalam persekitaran aplikasi web bagi SNE Sdn. Bhd.*

[4 marks]
[*4 markah*]

QUESTION 2

SOALAN 2

CLO1 (a)(i) Figure B2(a)(i) illustrates the Security Settings for a folder named "My Folder". Describe **TWO (2)** types of permission for files and folders that help maintain security and protect sensitive and important data from unauthorized access or alterations.

*Rajah B2(a)(i) menunjukkan contoh Tetapan Keselamatan untuk folder yang dinamakan "My Folder". Terangkan **DUA (2)** jenis kebenaran untuk fail dan folder yang membantu mengekalkan keselamatan serta melindungi data sensitif dan penting daripada akses atau pengubahan yang tidak dibenarkan.*

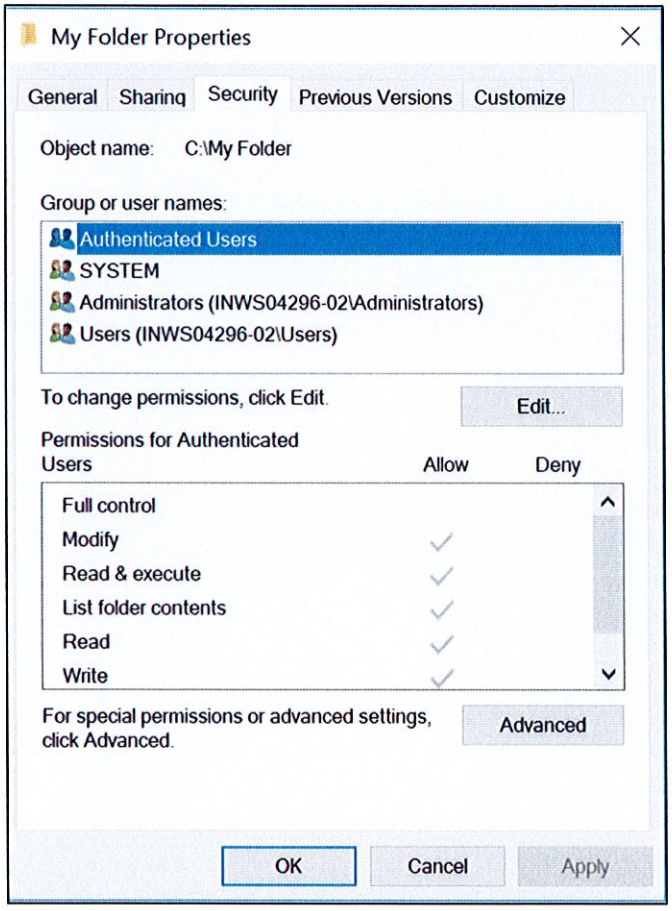

Figure B2(a)(i) / *Rajah B2(a)(i)*

[6 marks]

[*6 markah*]

CLO1

(a)(ii) Security Procedures and Policies are a collection of rules and guidelines that organizations establish to safeguard their information, assets, and resources from a range of threats, including cyber-attacks, data breaches, and unauthorized access. Explain the following policies that an organization can put in place.

Prosedur dan Polisi Keselamatan adalah sekumpulan peraturan dan garis panduan yang ditetapkan oleh organisasi untuk melindungi maklumat, aset, dan sumber mereka daripada pelbagai ancaman, termasuk serangan siber, kebocoran data, dan akses tanpa kebenaran. Huraikan polisi berikut yang boleh dilaksanakan oleh sesebuah organisasi.

- Ethics policy
  Polisi etika

- Hiring policy
  Polisi pengambilan

- Physical access control policies
  Polisi kawalan akses fizikal

- Separation duties policy
  Polisi pemisahan tugas

[8 marks]
[*8 markah*]

CLO1

(a)(iii) A security policy is a detailed framework of rules and procedures aimed at safeguarding an organization's information and technology assets against diverse security threats. Apply **FOUR (4)** best practices for managing usernames and passwords effectively.

*Polisi keselamatan adalah rangka kerja terperinci bagi peraturan dan prosedur yang bertujuan untuk melindungi maklumat dan aset teknologi organisasi daripada pelbagai ancaman keselamatan. Kenal pasti **EMPAT (4)** aplikasi amalan terbaik untuk pengurusan nama pengguna dan kata laluan dengan berkesan.*

[8 marks]
[*8 markah*]

CLO1

(b) The five pillars of information assurance are fundamental principles that ensure the protection and reliability of information systems. These pillars are designed to safeguard data from threats, ensure it is accessible to authorized users, and maintain its integrity. Describe any **FOUR (4)** pillars of information assurance.

*Lima tiang asas jaminan maklumat adalah prinsip-prinsip asas yang memastikan perlindungan dan kebolehpercayaan sistem maklumat. Tiang-tiang ini direka untuk melindungi data daripada ancaman, memastikan ia boleh diakses oleh pengguna yang dibenarkan, dan mengekalkan integritinya. Huraikan mana-mana **EMPAT (4)** tiang jaminan maklumat.*

[8 marks]
[*8 markah*]

SOALAN TAMAT