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 A : 45 MARKS
BAHAGIAN A : 45 MARKAH

INSTRUCTION:
This section consists of **THIRTY (30)** objective questions. Mark your answers in the OMR form provided.

ARAHAN:
*Bahagian ini mengandungi **TIGA PULUH (30)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1 1. Define the primary goal of cybersecurity.
Nyatakan matlamat utama keselamatan siber.

A. To develop software applications
Untuk membangunkan aplikasi perisian

B. To design hardware systems
Untuk mereka bentuk sistem perkakasan

C. To protect systems, networks, and programs
Untuk melindungi sistem, rangkaian, dan program

D. To create new programming languages
Untuk mencipta bahasa pengaturcaraan baharu

CLO1 2. Identify the **CORRECT** criteria of Unstructured Security Threat.
*Kenal pasti kriteria Ancaman Keselamatan Berstruktur yang **BETUL**.*

A. Hackers know system vulnerabilities
Penggodam mengetahui kelemahan sistem

B. Testing and challenging a hacker's skills
Menguji dan mencabar kemahiran penggodam

C. Hackers can understand and develop code and exploit scripts
Penggodam dapat memahami dan mengembangkan kod dan skrip eksploitasi

D. Hackers understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses
Penggodam memahami, mengembangkan, dan menggunakan teknik penggodaman yang canggih untuk menembusi perniagaan yang tidak curiga

CLO1

3. Define vulnerability in the context of a network or device.
Takrifkan kerentanan dalam konteks rangkaian atau peranti.

A. The speed of data transfer
Kelajuan pemindahan data

B. The degree of strength in a network
Tahap kekuatan dalam rangkaian

C. The level of access granted to users
Tahap akses yang diberikan kepada pengguna

D. The degree of weakness in a network or device
Tahap kelemahan dalam rangkaian atau peranti

CLO1

4. Select the **CORRECT** source for a security threat caused by an employee who unintentionally clicks on a phishing email.
*Pilih sumber yang **BETUL** untuk ancaman keselamatan yang disebabkan oleh tindakan seorang pekerja yang tanpa sengaja mengklik pada emel "phishing".*

A. External and structured
Luaran dan berstruktur

B. Internal and unstructured
Dalaman dan tidak berstruktur

C. External and unstructured
Luaran dan tidak berstruktur

D. Internal and structured
Dalaman dan berstruktur

CLO1 5. Identify the type of security attack where the attacker actively alters the system.
Kenal pasti jenis serangan keselamatan di mana penyerang secara aktif mengubah sistem.

A. Passive Attack
Serangan Pasif

B. Active Attack
Serangan Aktif

C. Close-in Attack
Serangan Dekat

D. Distribution Attack
Serangan Pengedaran

CLO1 6. Select the **CORRECT** phase in the Cyber Kill Methodology Flow that involves sending malicious payload to the target.
*Pilih fasa yang **BETUL** dalam Metodologi Pembunuhan Siber Aliran melibatkan penghantaran muatan jahat kepada sasaran.*

A. Delivery
Penyampaian

B. Weaponization
Penggunaan Senjata

C. Command and Control
Perintah dan Kawalan

D. Actions on Objective
Tindakan ke atas Objektif

CLO1 7. Identify the impersonation-based social engineering techniques that involve listening in on conversation to collect sensitive information.
Kenal pasti teknik kejuruteraan sosial berasaskan penyamaran yang melibatkan mendengar perbualan untuk mengumpul maklumat sensitif.

A. Quid Pro Quo
Timbal balik

B. Piggybacking
Menumpang

C. Dumpster diving
Menggali tong sampah

D. Eavesdropping
Mendengar secara diam-diam

CLO1 8. Select the **CORRECT** statement that best interpret a Reconnaissance Attack.
*Pilih kenyataan yang **BETUL** yang paling tepat menginterpretasikan Serangan Pengintipan.*

A. It involves overwhelming a server with traffic to disrupt its services
Ia melibatkan membanjiri pelayan dengan trafik untuk mengganggu perkhidmatannya

B. It is a technique used to exploit a vulnerability in software to gain unauthorized access
Ia adalah teknik yang digunakan untuk mengeksploitasi kelemahan dalam perisian bagi mendapatkan akses tanpa kebenaran

C. It refers to the use of malware to damage or disrupt a system
Ia merujuk kepada penggunaan perisian malware untuk merosakkan atau mengganggu sistem

D. It aims to gather information about a target system or network without causing harm
Ia bertujuan untuk mengumpul maklumat tentang sistem atau rangkaian sasaran tanpa menyebabkan sebarang kerosakan

CLO1

9. Express the **BEST** explanation that characterises phishing emails.
*Nyatakan penjelasan **TERBAIK** yang menggambarkan emel "phishing".*

A. Email that contains malicious links or attachments aimed at tricking the recipient into providing sensitive information
Emel yang mengandungi pautan atau lampiran berniat jahat yang bertujuan untuk menipu penerima agar memberikan maklumat sensitif

B. Legitimate emails sent by trusted organizations to verify account information
Emel yang sah yang dihantar oleh organisasi yang dipercayai untuk mengesahkan maklumat akaun

C. Notifications email from internet service providers regarding service upgrades
Pemberitahuan emel daripada penyedia perkhidmatan internet mengenai peningkatan perkhidmatan

D. Email that contains information about software updates that need to be installed immediately
Emel yang mengandungi maklumat tentang kemas kini perisian yang perlu dipasang dengan segera

CLO1

10. Select the **CORRECT** category for Google Chrome under IT infrastructure.
*Pilih kategori yang **BETUL** untuk Google Chrome di bawah infrastruktur IT.*

A. Data
Data

B. Application
Aplikasi

C. Network
Rangkaian

D. Physical
Fizikal

CLO1

11. Identify the purpose of the Security Baseline in infrastructure security.
Kenal pasti tujuan Rujukan Keselamatan dalam keselamatan infrastruktur.

A. The process of applying security patches
Proses memohon tampalan keselamatan

B. Monitoring network traffic
Memantau trafik rangkaian

C. A standard set of security configurations
Set standard konfigurasi keselamatan

D. Installing security hardware
Memasang perkakasan keselamatan

CLO1

12. Select the function of Honeypot in network security.
Pilih fungsi Honeypot dalam keselamatan rangkaian.

A. It strengthens encryption protocols for secure data transmission
Ia menguatkan protokol penyulitan untuk penghantaran data yang selamat

B. It blocks unauthorized access to a private network
Ia menghalang akses tidak sah ke rangkaian peribadi

C. It scans and detects vulnerabilities in network devices
Ia mengimbas dan mengesan kelemahan dalam peranti rangkaian

D. It attracts and traps potential attackers to study their behaviour
Ia menarik dan menjebak penyerang yang berpotensi untuk mengkaji tingkah laku mereka

CLO1

13. Identify the **CORRECT** statement that describes the roles of antivirus in defending against malware.
*Kenal pasti pernyataan yang **BETUL** yang menerangkan peranan perisian antivirus dalam melindungi daripada perisian hasad.*

A. Antivirus software detects, prevents, and removes malicious software from the computer
Perisian antivirus mengesan, mencegah, dan menghapuskan perisian berniat jahat dari komputer

B. Antivirus software primarily focuses on monitoring network traffic for suspicious activities
Perisian antivirus terutamanya memberi tumpuan kepada memantau trafik rangkaian untuk aktiviti yang mencurigakan

C. Antivirus software is used to encrypt data to prevent unauthorized access
Perisian antivirus digunakan untuk menyulitkan data bagi mengelakkan akses tanpa kebenaran

D. Antivirus software creates backups of files to protect them from being corrupted by malware
Perisian antivirus membuat salinan fail untuk melindungi mereka daripada rosak akibat perisian hasad

CLO1

14. Select the statement that explains the role of access control methods in protecting physical computer and network equipment.
Pilih kenyataan yang menerangkan peranan kaedah kawalan akses dalam melindungi peralatan komputer dan rangkaian fizikal.

A. Solely focus on monitoring network traffic for suspicious activities.
Hanya memberi tumpuan kepada pemantauan trafik rangkaian untuk aktiviti yang mencurigakan.

B. Prevent unauthorized access by implementing physical barriers and biometric authentication techniques.
Mencegah akses tanpa kebenaran dengan melaksanakan halangan fizikal dan teknik pengesahan biometrik.

C. Provide fire suppression systems to protect equipment from environmental hazards.
Menyediakan sistem pemadam kebakaran untuk melindungi peralatan daripada bahaya alam sekitar.

D. Enhance the wireless network performance by managing signal strength and interference.
Meningkatkan prestasi rangkaian tanpa wayar dengan mengurus kekuatan isyarat dan gangguan.

CLO1

15. Based on the statement below, determine the application security hardening method that should be used in this scenario.
Berdasarkan kenyataan di bawah, tentukan kaedah pengukuhan keselamatan aplikasi yang harus digunakan dalam scenario ini.

> An organization aims to enhance the stability and security of its software by installing a comprehensive update that contains several fixes and improvements.
> *Sebuah organisasi berhasrat untuk meningkatkan kestabilan dan keselamatan perisian mereka dengan memasang kemas kini menyeluruh yang mengandungi beberapa pembaikan dan penambahbaikan.*

A. Service Pack
Pek Perkhidmatan

B. Hotfix
Pembaikan segera

C. Bug Fix
Pembaikan pepijat

D. Cold Fix
Pembaikan sejuk

CLO1

16. Identify the key aspects of information security policy governance and management that organizations need to understand.
Kenal pasti aspek utama dalam tadbir urus dan pengurusan dasar keselamatan maklumat yang perlu difahami oleh organisasi.

A. Budgeting for office renovations
Menganggarkan bajet untuk pengubahsuaian pejabat

B. Increasing social media presence
Meningkatkan kehadiran di media sosial

C. Developing creative marketing campaigns
Membangunkan kempen pemasaran kreatif

D. Compliance with information security laws and regulations
Pematuhan terhadap undang-undang dan peraturan keselamatan maklumat

CLO1 17. Select the **CORRECT** statement that describes the purpose of information classification in an organization.
*Pilih pernyataan yang **BETUL** yang menerangkan tujuan pengelasan maklumat dalam sesebuah organisasi.*

A. To allocate budgetary resources to different departments
Untuk memperuntukkan sumber bajet kepada jabatan yang berbeza

B. To organize files based on their creation data for easier retrieval
Untuk mengatur fail berdasarkan tarikh penciptaan mereka untuk memudahkan pencarian

C. To determine the marketing strategy for different customer segments
Untuk menentukan strategi pemasaran untuk segmen pelanggan yang berbeza

D. To categorize information based on its level of sensitivity and importance
Untuk mengkategorikan maklumat berdasarkan tahap sensitiviti dan kepentingannya

CLO1 18. Identify the primary purpose of a security policy document within an organization.
Kenal pasti tujuan utama dokumen dasar keselamatan dalam sesebuah organisasi.

A. To arrange work schedules and employee leave
Untuk mengatur jadual kerja dan cuti pekerja

B. To provide information about financial procedures and regulations
Untuk menyediakan maklumat mengenai prosedur dan peraturan kewangan

C. To outline the organization's procedures for handling and protecting sensitive information
Untuk menggariskan prosedur organisasi untuk menangani dan melindungi maklumat sensitif

D. To provide guidelines for employee about office code of ethics
Untuk menyediakan garis panduan kepada pekerja mengenai kod etika pejabat

CLO1

19. Select the **BEST** description for the purpose of Hiring Policies within an organization.
*Pilih yang **PALING TEPAT** menerangkan tujuan Polisi Pengambilan dalam sesebuah organisasi.*

A. To ensure a consistent and fair process for recruiting and selecting candidates
Untuk memastikan proses yang konsisten dan adil dalam merekrut dan memilih calon

B. To outline the procedures of selecting the top management
Untuk menggariskan prosedur pemilihan pengurusan tertinggi

C. To provide guidelines for marketing strategies and brand development
Untuk menyediakan garis panduan bagi strategi pemasaran dan pembangunan jenama

D. To specify requirements for employee performance evaluations
Untuk menentukan keperluan bagi nilai prestasi pekerja

CLO1

20. Figure A20 illustrates an example of a fingerprint scanner. Select the **CORRECT** answer regarding how biometrics contribute to data protection within an organization.
*Rajah A20 menggambarkan contoh pengimbas cap jari. Pilih jawapan yang **BETUL** mengenai bagaimana biometrik membantu melindungi data dalam sesebuah organisasi.*

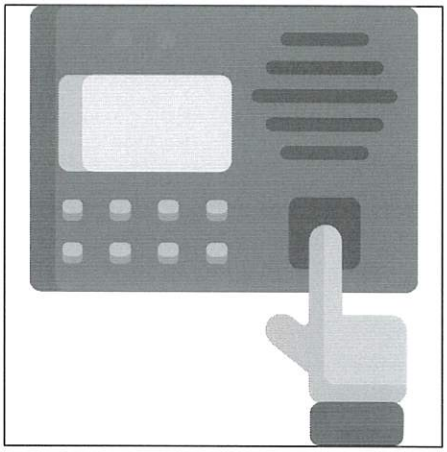

Figure A20 / Rajah A20

A. By analyzing data to predict future trends
Dengan menganalisis data untuk meramalkan trend masa depan

B. By organizing data into different security levels
Dengan mengatur data ke dalam tahap keselamatan yang berbeza

C. By increasing the speed of data processing
Dengan meningkatkan kelajuan pemprosesan data

D. By verifying user's unique physical traits to ensure only authorized user can access data
Dengan mengesahkan ciri fizikal unik pengguna untuk memastikan hanya pengguna yang sah boleh mengakses data

CLO2

21. Select the purpose of Multi-Factor Authentication (MFA) in enhancing security.
Pilih tujuan Multi-Factor Authentication (MFA) dalam meningkatkan keselamatan.

A. Speed ups the login process with just one method of authentication
Mempercepatkan proses log masuk dengan hanya satu kaedah pengesahan

B. Allows users to access their accounts using only a single password
Membenarkan pengguna mengakses akaun mereka dengan hanya satu kata laluan

C. Requires user to provide two or more types of verification to access their accounts
Memerlukan pengguna untuk memberikan dua atau lebih jenis pengesahan untuk mengakses akaun mereka

D. Helps to organize user accounts into different access levels without extra verification
Membantu mengatur akaun pengguna ke dalam tahap akses yang berbeza tanpa pengesahan tambahan

CLO1

22. An employee is leaving the company, and you as an IT Manager need to ensure his access to sensitive systems is revoked. Identify the security policy guides in this process.
Seorang pekerja akan meninggalkan syarikat, dan anda sebagai Pengurus IT perlu memastikan akses mereka ke sistem sensitif ditarik balik. Kenal pasti panduan dasar keselamatan dalam proses ini.

A. Termination policies
Polisi pemberhentian

B. Ethics policy
Polisi etika

C. Acceptable use policy
Polisi penggunaan yang boleh diterima

D. Separation duties policies
Polisi pemisahan tugas

CLO1 23. To ensure all the sensitive documents are securely disposed of so that they cannot be accessed by unauthorized users, choose a policy that addresses this requirement.
Untuk memastikan semua dokumen sensitif dilupuskan dengan selamat, supaya tidak boleh diakses oleh pengguna yang tidak sah, pilih dasar yang menangani keperluan ini.

A. Hiring policies
Polisi pemgambilan

B. Document disposal and destruction policies
Polisi pelupusan dan pemusnahan dokumen

C. Termination policies
Polisi pemberhentian

D. Separation duties policies
Polisi pemisahan tugas

CLO1 24. Figure A24 illustrates the critical processes utilized by FinTech Az Corp. Ali, the company's CEO, aims to reduce the risk of conflicts of interest within the organization. Determine a policy that should be applied to these critical processes.
Rajah A24 menunjukkan proses-proses kritikal yang digunakan oleh FinTech Az Corp. Ali, sebagai CEO syarikat, ingin mengurangkan risiko konflik kepentingan dalam syarikatnya. Tentukan polisi yang perlu diterapkan pada proses-proses kritikal ini.

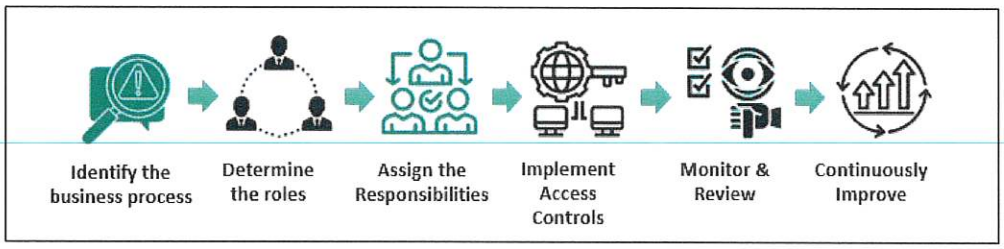

Figure A24 / *Rajah A24*

A. Hiring policies
Polisi pengambilan

B. Separation duties policies
Polisi pemisahan tugas

C. Ethics policies
Polisi etika

D. Need-to-know policies
Polisi keperluan untuk tahu

CLO1 25. You as an IT Manager need to assign administrative rights to a new IT team member who requires access to multiple systems. Determine the method that **BEST** demonstrates privilege management.
*Anda sebagai Pengurus IT perlu memberikan hak pentadbiran kepada ahli pasukan IT baru yang memerlukan akses kepada pelbagai sistem. Tentukan kaedah yang **PALING BAIK** menunjukkan pengurusan hak istimewa.*

A. Adding the user to an administrative group and configuring group policies
Menambah kata laluan sementara kepada pengguna untuk mengkonfigurasi dasar kumpulan

B. Sending the user a temporary password to access systems
Menghantar kata laluan sementara kepada pengguna untuk mengakses sistem.

C. Providing the user with physical access to the server room
Memberikan akses fizikal kepada pengguna ke bilik pelayan

D. Allowing the user to request permissions as needed
Membenarkan pengguna untuk meminta kebenaran mengikut permintaan

CLO1 26. A company wants to ensure that only authorized personnel can access sensitive financial data. Determine an effective privilege management practice to achieve this situation.
Sebuah syarikat ingin memastikan hanya kakitangan yang dibenarkan sahaja boleh mengakses data kewangan yang sensitif. Tentukan amalan pengurusan hak istimewa yang berkesan untuk mencapai situasi ini.

A. Distributing the financial data on shared drive for easy access
Mengedarkan data kewangan di pemacu bersama untuk akses yang mudah

B. Implementing role-based access control (RBAC) and regularly reviewing access permission
Melaksanakan kawalan akses berdasarkan peranan (RBAC) dan menyemak kebenaran akses secara berkala

C. Using the same password for all financial system
Menggunakan kata laluan yang sama untuk semua sistem kewangan

D. Providing unrestricted access to all employees for ease of collaboration
Memberi akses tanpa had kepada semua pekerja untuk memudahkan kerjasama

CLO1 27. Identify the primary difference between information assurance and information security.
Kenal pasti perbezaan utama antara jaminan maklumat dan keselamatan maklumat.

A. Information assurance involves creating policies, while information security involves technical measures
Jaminan maklumat melibatkan penciptaan polisi, sementara keselamatan maklumat melibatkan langkah-langkah teknikal

B. Information assurance and information security are the same and can be used interchangeably
Jaminan maklumat dan keselamatan maklumat adalah perkara yang sama dan boleh digunakan secara bergantian

C. Information assurance ensures the reliability and availability of information, while information security protects information from unauthorized access and threats
Jaminan maklumat memastikan kebolehpercayaan dan ketersediaan maklumat, sementara keselamatan maklumat melindungi maklumat daripada akses tanpa izin dan ancaman

D. Information assurance emphasizes availability, integrity, and confidentiality while information security only focuses on preventing unauthorized access
Jaminan maklumat menekankan ketersediaan, integrity, dan kerahsiaan, manakala keselamatn maklumat hanya menekankan menghalang akses tanpa izin

CLO1 28. Select the purpose of computer laws in information assurance.
Pilih tujuan undang-undag computer dalam jaminan maklumat.

A. To enforce copyright on books and films
Untuk menguatkuasakan hak cipta ke atas buku dan filem

B. To control the sale of computer hardware
Untuk mengawal jualan perkakasan komputer

C. To establish physical security standards for offices
Untuk menetapkan piawaian keselamatan fizikal bagi pejabat

D. To regulate the use of computers and digital data to prevent cybercrimes
Untuk mengawal penggunaan computer dan data digital bagi mencegah jenayah siber

CLO1 29. Identify the following that is **NOT** typically covered under intellectual property laws.
*Kenal pasti yang berikut **TIDAK** biasanya dilindungi di bawah undang-undag harta intelek.*

A. Patents
Paten

B. Copyrights
Hak Cipta

C. Trademarks
Tanda dagangan

D. Personal Data Privacy
Privasi Data Peribadi

CLO1 30. Select the privacy law that is primarily aim to protect.
Pilih undang-undang privasi yang tujuan utamanya untuk melindungi.

A. The financial transactions of corporations
Transaksi kewangan korporat

B. The personal information and privacy of individuals
Maklumat peribadi dan privasi individu

C. The intellectual property of businesses
Harta intelek perniagaan

D. The environmental standards of a country
Piawaian alam sekitar sesebuah negara

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.*

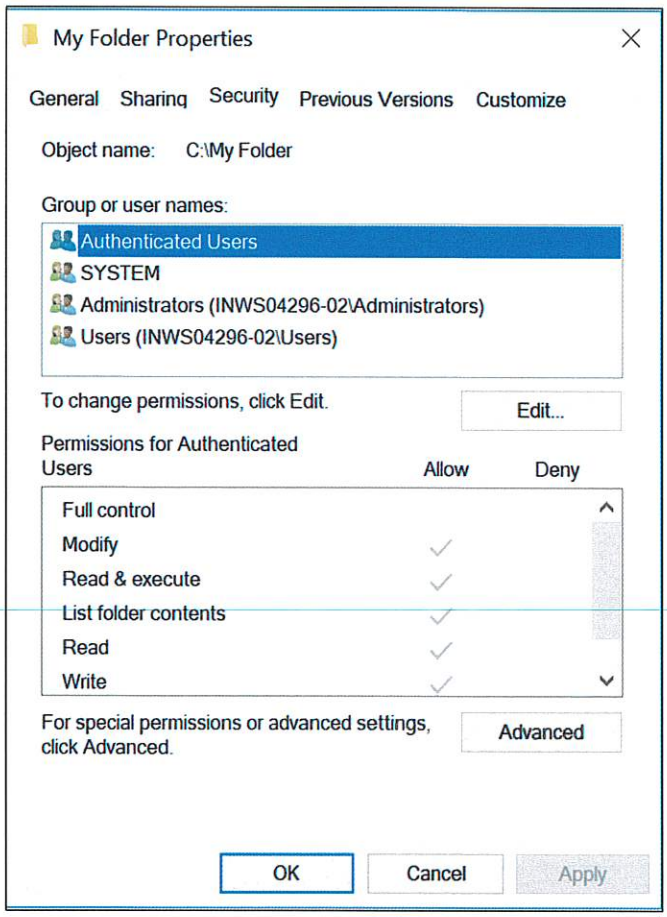

Figure B2(a)(i) / *Rajah B2(a)(i)*

[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