

SULIT



**BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI
KEMENTERIAN PENDIDIKAN MALAYSIA**

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

**PEPERIKSAAN AKHIR
SESI JUN 2019**

DFT4013: SECURITY BASICS AND IT PROFESIONAL

**TARIKH : 02 NOVEMBER 2019
MASA : 2.30 PETANG - 4.30 PETANG (2 JAM)**

Kertas ini mengandungi **DUA PULUH SATU (21)** halaman bercetak.

Bahagian A: Objektif (30 soalan)

Bahagian B: Struktur (2 soalan)

Dokumen sokongan yang disertakan : Tiada

JANGAN BUKA KERTAS SOALANINI SEHINGGA DIARAHKAN

(CLO yang tertera hanya sebagai rujukan)

SULIT

SECTION A : 45 MARKS
BAHAGIAN A : 45 MARKAH

INSTRUCTION:

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

ARAHAN :

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

- | | |
|------------|---|
| CLO1
C1 | <p>1. Identify the term of electronic message systems that send out unrequested or unwanted messages in bulk to a large number of recipients.
<i>Kenal pasti istilah sistem mesej elektronik yang menghantar mesej yang tidak ditanyakan atau tidak diinginkan secara pukal kepada sejumlah besar penerima.</i></p> <p>A. Spam
B. Hashing
C. Phishing
D. Encryption</p> |
| CLO1
C2 | <p>2. Digital signature is a special type of data safety maintenance where a special kind of signature is required to access some particular information. Identify the consequences if unauthorized user accesses the data without digital signature.
<i>Tandatangan digital adalah sejenis penyelenggaraan keselamatan data khas di mana jenis tanda tangan khas diperlukan untuk mengakses beberapa maklumat tertentu. Kenal pasti akibatnya jika pengguna tidak dibenarkan mengakses data tanpa tandatangan digital.</i></p> <p>A. The availability of the information is guaranteed
<i>Ketersediaan maklumat dijamin</i></p> <p>B. The confidentiality of the information is guaranteed
<i>Kerahsiaan maklumat tersebut dijamin</i></p> <p>C. The integrity of the information is no longer guaranteed
<i>Integriti maklumat tidak lagi dijamin</i></p> <p>D. The availability of the information is no longer guaranteed
<i>Ketersediaan maklumat tidak lagi dijamin</i></p> |

CLO1 C1	3.	Identify the biometric security device. <i>Kenal pasti peranti keselamatan biometrik.</i>
	A.	Key fob <i>Fob kunci</i>
	B.	Fingerprint <i>Cap jari</i>
	C.	RFID card <i>Kad RFID</i>
	D.	Password <i>Katalaluan</i>
CLO1 C2	4.	Select the strongest password that can be used for a system. <i>Pilih kata laluan terkuat yang boleh digunakan untuk sistem.</i>
	A.	AbCDe123!
	B.	PAssWoRD
	C.	D+11L4N0v@
	D.	qwertyuiopasd
CLO1 C3	5.	Encik Rizal is a lecturer who teaches the DFT4013 course and he wants to share the note folders with his students where students can view only. Choose which file permission level that can fulfill his requirement. <i>Encik Rizal merupakan pensyarah yang mengajar subjek DFT4013 dan beliau hendak berkongsi nota dengan pelajarnya dimana pelajar hanya boleh melihat sahaja. Pilih tahap kebenaran fail yang boleh memenuhi keperluan tersebut.</i>
	A.	Write <i>Tulis</i>
	B.	Read <i>Baca</i>
	C.	Modify <i>Ubahsuai</i>
	D.	Full Control <i>Kawalan Penuh</i>

- CLO1 C3 6. Puan Liza has attended a course at company CyberSecurity Sdn Bhd. As a visitor, she needs access to email, the internet and network printer there. As a network administrator, choose the type of account that can be given to her.
Puan Liza telah menghadiri satu kursus di syarikat CyberSecurity Sdn Bhd. Sebagai pelawat, beliau memerlukan akses kepada e-mail, internet dan pencetak rangkaian disana. Sebagai pentadbir rangkaian, pilih jenis akaun yang boleh diberikan kepada beliau.
- A. Guest account
Akaun tetamu
 - B. User account
Akaun pengguna
 - C. Standard account
Akaun standard
 - D. Administrator account
Akaun pentadbir
- CLO2 C1 7. Identify “Security Policies” definition in terms of small business planning.
Kenal pasti definisi "Dasar Keselamatan" dari segi perancangan perniagaan kecil
- A. Any event that impairs the ability of an organization to continue operating
Mana-mana kejadian yang mengurangkan keupayaan organisasi untuk meneruskan operasi
 - B. Using natural event that impairs the ability of an organization to continue operating
Menggunakan kejadian semula jadi yang mengurangkan keupayaan organisasi untuk meneruskan operasi
 - C. Using man-made event that impairs the ability of an organization to continue operating
Menggunakan kejadian buatan manusia yang mengurangkan keupayaan organisasi untuk meneruskan operasi
 - D. Using desktop security products such as antivirus, antispam and firewalls, network intrusion detection, and hardware technologies
Menggunakan produk keselamatan desktop seperti antivirus, antispam dan firewall, pengesanan pencerobohan rangkaian, dan teknologi perkakasan teknologi.

- CLO2 C2 8. Choose the **BEST** answer to describe about structured threats.
Pilih jawapan yang TERBAIK bagi menerangkan mengenai ancaman berstruktur.
- A. Arise from individuals or organizations working outside of a company
Wujud daripada individu atau organisasi yang bekerja di luar syarikat
- B. Come from hackers that are more highly motivated and technically competent
Datang daripada penggodam yang lebih bermotivasi dan kompeten dari segi teknikal
- C. Occur when someone has authorized access to the network with an account on server or physical access to network
Berlaku apabila seseorang telah diberi kuasa akses kepada rangkaian dengan akaun di server atau akses fizikal kepada rangkaian
- D. Consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers
Terdiri daripada individu yang kebanyakannya tidak berpengalaman dan menggunakan alat-alat penggodaman yang mudah didapati seperti 'shell script' dan penggodam kata laluan.
- CLO2 C3 9. Hasannah try to delete one folder in office PC, but the result shows "Folder Access Denied".
Hasannah cuba memadamkan satu folder di PC pejabat, tetapi terdapat paparan menunjukkan "Akses Folder Ditolak".
- Choose the **CORRECT** method to solve the problem above.
Pilih cara yang TEPAT untuk selesaikan masalah di atas.
- A. Signature File Updates
Kemas kini signature fail
- B. Principle of Least Privilage
Prinsip Keistimewaan Sedikit
- C. Restricting User Permission
Menghadkan Kebenaran Pengguna
- D. Protecting Against Malicious Software
Melindungi Terhadap Perisian Bahaya

- CLO1 C1 10. Identify the name of the decrypted form of the message.
Kenal pasti nama mesej yang telah dinyahsulitkan.
- A. Plaintext
B. Wordtext
C. Formtext
D. Ciphertext
- CLO1 C2 11. Classify the encryption key that spread to all users who want to send encrypted message.
Klasifikasikan kunci penyulitan yang tersebar ke semua pengguna yang mahu menghantar mesej penyulitan.
- A. Private key
Kunci Sulit
- B. Public key
Kunci Awam
- C. Secret key
Kunci Rahsia
- D. Symmetric key
Kunci Simetri
- CLO1 C3 12. A network administrator has a problem when the SSID broadcast has been disabled on the computer. Choose a method to help in solving this problem.
Pentadbir rangkaian mempunyai masalah apabila SSID broadcast telah dinyaah aktifkan pada komputer. Pilih kaedah untuk membantunya menyelesaikan masalah ini.
- A. Manually enter the SSID on the computer
Masukkan SSID secara manual pada komputer.
- B. Turn ON or ENABLE the SSID on the wireless device.
HIDUPKAN atau AKTIFKAN SSID pada peranti tanpa wayar.
- C. Change the router security mode to WPA2 rather than WEP mode.
Tukar mod keselamatan router ke WPA2 dan bukannya mod WEP.
- D. Configure the wireless router by ensuring the computer MAC address.
Konfigurasi router tanpa wayar dengan memastikan alamat MAC komputer.

- CLO1 13. **Figure A13** shows an example of a full cipher alphabet . Based on the figure, apply the ciphertext for statement “ U ARE REALLY GOOD ”
Rajah A13 menunjukkan abjad cipher lengkap. Berdasarkan rajah tersebut, hasilkan ciphertext untuk pernyataan " U ARE REALLY GOOD ".

Plain alphabet:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
-----------------	----------------------------

Cipher alphabet:	DEFGHIJKLMNOPQRSTUVWXYZABC
------------------	----------------------------

Figure A13 / Rajah A13

- A. X EVI KIPPYS FTMG
- B. X EVI KIPPYM FWMG
- C. X DUH UHDHOOB JRRG
- D. X DUH JHILOOB EDRG

- CLO2 14. Identify the security practice to protect wireless router from dictionary attack.
Kenal pasti amalan keselamatan untuk melindungi router rangkaian tanpa wayar dari serangan kamus.

- A. Power on WPS
Buka WPS
- B. Turn off WPS
Matikan WPS
- C. Disable SSID
Memadam SSID
- D. Change to WEP mode
Tukar ke WEP mode

- CLO2 15. Select the wireless configuration features that can prevent wireless device from connecting to the network if the device do not have an authorized physical address.
Pilih konfigurasi tanpa wayar yang boleh menghalang peranti tanpa wayar daripada menyambung ke rangkaian jika peranti tidak mempunyai alamat fizikal yang dibenarkan.

- A. Enabling the proxy firewall
Membenarkan proxy firewall
- B. Disabling SSID broadcasts
Melumpuhkan penyebaran SSID

- C. Disabling port forwarding
Melumpuhkan port forwarding
- D. Enabling MAC address filtering
Membenarkan penapisan alamat MAC
- CLO2 C3 16. An attacker wants to hack the wireless router and realise that SSID broadcast is disabled. Identify the solutions the attacker should applied to accomplished her mission.
Seorang penyerang mahu menggodam router tanpa wayar dan menyedari bahawa penyiaran SSID dilumpuhkan. Kenal pasti penyelesaian lain yang perlu dilaksanakan oleh penyerang untuk mencapai misi beliau.
- A. Use internet access connection
Guna perhubungan akses internet
- B. Find the wireless network name
Cari nama rangkaian tanpa wayar
- C. Use multicast wireless network
Guna multicast rangkaian tanpa wayar
- D. Collect data using wireless cracker
Kumpul data menggunakan cracker rangkaian tanpa wayar
- CLO2 C3 17. User needs to upload a large size file on web. Choose the fastest encryption method for this situation.
Pengguna perlu memuat naik fail saiz besar di web. Pilih kaedah penyulitan terpantas untuk keadaan ini.
- A. Public encryption
Penyulitan awam
- B. Hash encryption
Penyulitan hashing
- C. Symmetric encryption
Penyulitan simetri
- D. Asymmetric encryption
Penyulitan tidak simetri

- CLO2 C4
18. Classify the security threats using credit card in cybercriminal.
Klasifikasikan ancaman keselamatan menggunakan kad kredit dalam jenayah siber.
- I. Malware
Malware
- II. Pishing
Memancing
- III. Data Stolen
Kecurian Data
- IV. Insecure Practice
Amalan tidak selamat
- A. I only
- B. I and II
- C. I, II and III
- D. I, II, III and IV
- CLO1 C1
19. Identify the next steps of troubleshooting process that a technician must take after identify the customer problems.
Kenal pasti langkah seterusnya bagi proses penyelesaian masalah yang mesti diambil oleh juruteknik selepas mengenal pasti masalah pelanggan.
- A. Establish a plan of action.
Mewujudkan pelan tindakan.
- B. Verify full system functionality.
Sahkan fungsi sistem penuh.
- C. Document findings, actions, and outcomes
Dokumentasi penemuan, tindakan dan hasil.
- D. Establish a theory of probable causes.
Mewujudkan satu teori kemungkinan penyebabnya.

- CLO1 C2 20. Mr Ooi receives a phone call from a customer that asks about device warranty but he does not getting any information from her. Classify the type of customer. *Encik Ooi menerima panggilan telefon dari seorang pelanggan yang bertanyakan berkaitan produk waranti tetapi dia tidak memperolehi sebarang maklumat daripadanya. Klasifikasikan jenis pelanggan tersebut.*
- Rude
Biadap
 - Happy
Gembira
 - Talkative
Bercakap banyak
 - Inexperience
Kurang Pengalaman
- CLO1 C3 21. Choose why the technician must prepare a document after solving a customer problem.
Pilih mengapakah juruteknik mesti menyediakan dokumentasi selepas menyelesaikan masalah pengguna.
- To be given to senior technician as a journal report
Untuk diberikan kepada juruteknik kanan sebagai laporan jurnal
 - For further research if same problem have occur
Untuk penyelidikan lanjut jika masalah yang sama berlaku
 - To show that the problem already solved
Untuk menunjukkan bahawa masalah telah diselesaikan
 - To make an analysis and try to find another solutions
Membuat analisa dan cuba mencari penyelesaian lain
- CLO2 C3 22. Choose the effect of Malware Attack in e-mail delivery.
Pilih kesan serangan Malware di dalam penghantaran e-mel.
- A virus using user account to send spam and delivery failure
Virus menggunakan akaun pengguna untuk menghantar spam dan kegagalan penghantaran emel
 - A virus using user account to send spam and email is successfully sent.
Virus menggunakan akaun pengguna untuk menghantar spam dan emel berjaya di hantar

- C. A virus attacking network and slowing network connection
Virus menyerang rangkaian dan menjadikan sambungan rangkaian lambat
- D. A virus capturing transmitted data packets and decoding the packet's raw data
Virus menangkap paket data yang dihantar dan mengubah paket data asal
- CLO2 C3 23. A hacker uses an available wireless hacking tool to crack the 128-bit WEP. Choose the correct solution for this issue.
Seorang penggodam menggunakan alat penggodam tanpa wayar untuk memecahkan WEP 128-bit. Pilih penyelesaian yang betul untuk isu ini.
- A. Change to WPA encryption
Tukar kepada penyulitan WPA
- B. Upgrade antenna wireless
Naik taraf antenna tanpa wayar
- C. Update database encryption
Kemaskini penyulitan pangkalan data
- D. Get a new wireless router
Dapatkan router tanpa wayar yang baru
- CLO2 C4 24. The USB drive of a management staff at Solaris Ltd had been infecting the network with viruses. Select the best solution to prevent the viruses from affecting other users.
Pemacu USB pengurusan kakitangan di Solaris Ltd telah menjangkiti rangkaian dengan virus. Pilih penyelesaian terbaik untuk mencegah virus daripada menjaskan pengguna lain.
- A. Implement account access security policy at the company.
Melaksanakan dasar keselamatan akses akaun di syarikat.
- B. Install client antivirus on workstation and disable virus definition update.
Pasang antivirus pelanggan pada stesen kerja dan nyahdayakan kemas kini definisi virus.
- C. Turn On Windows Firewall at all connected network workstations.
Hidupkan Windows Firewall di semua stesen kerja yang bersambung.
- D. Set antivirus software to scan removable media when data is accessed.
Tetapkan perisian antivirus untuk mengimbas media apabila data diakses.

CLO1 C3	<p>25. As a call center technician, show the proper way to keep a talkative customer focused on the problem that he is reporting. <i>Sebagai juruteknik panggilan pusat, tunjukkan cara yang betul untuk memastikan pelanggan banyak bercakap memberi tumpuan kepada masalah yang dia laporkan.</i></p> <p>I. Never interrupt a customer. <i>Jangan menyampuk pelanggan.</i></p> <p>II. Ask as many closed-ended questions as you need. <i>Tanya soalan-soalan tertutup yang anda perlukan.</i></p> <p>III. Put a customer in hold or transfer the call. <i>Letakkan pelanggan di talian atau pindahkan panggilan.</i></p> <p>IV. Gather as much information about the problem as possible. <i>Kumpulkan sebanyak mungkin maklumat mengenai masalah ini.</i></p> <p>A. I and II B. I and III C. II and III D. I, II and IV</p>
CLO1 C3	<p>26. A customer is angry and calls to complain about the service scheduled on the computer took longer than expected, and until now it is not yet solved. As a technician, you reviewed the work order and notices that the service was performed by a new employee. <i>Seorang pelanggan marah dan membuat panggilan untuk mengadu bahawa perkhidmatan yang dijadualkan pada komputer mengambil masa lebih lama daripada yang dijangkakan, dan sehingga sekarang masih belum selesai. Sebagai seorang juruteknik, anda merujuk perintah kerja dan menyedari bahawa perkhidmatan itu telah dilakukan oleh pekerja baru</i></p>

Based on the statement above, choose the proper response as a technician.
Berdasarkan penyataan di atas, pilih tindak balas yang betul sebagai seorang juruteknik.

- A. Put the customer on hold until a supervisor is available
Letakkan pelanggan di talian menunggu sehingga penyelia ada
- B. Verify that the computer is now working properly
Sahkan bahawa komputer berfungsi dengan baik sekarang

- C. Explain that the repair technician sent to perform the service is inexperienced
Menjelaskan bahawa juruteknik pemberian yang dihantar untuk melaksanakan perkhidmatan itu tiada berpengalaman
- D. Listen to the complaint and apologize for any inconvenience, then schedule a service for him by an experienced staff
Mendengar aduan itu dan meminta maaf atas sebarang kesulitan, kemudian jadualkan perkhidmatan untuk beliau oleh staf yang berpengalaman.
- CLO1 C3** 27. During the process of troubleshooting, a technician has gained access to customer private information. Choose the best way a technician should take to ensure the information is not being accessed by an unauthorized user.
Semasa proses menyelesaikan masalah, seorang juruteknik mendapat akses kepada maklumat peribadi pelanggan. Pilih tindakan terbaik juruteknik patut lakukan untuk memastikan informasi tersebut tidak boleh diakses oleh pengguna yang tidak sah.
- A. Documented all information in a log files.
Dokumentasi semua maklumat dalam fail log.
- B. Keep all confidential and follow security rules.
Simpan semua rahsia dan ikut peraturan keselamatan.
- C. Send this information to the technician manager.
Menghantar maklumat ini kepada pengurus juruteknik.
- D. Backup the information just in case customer needs it someday.
Backup maklumat sekiranya pelanggan memerlukannya suatu hari nanti.
- CLO1 C3** 28. Select actions that a technician should apply if illegal content is discovered on the hard drive of a customer computer.
Pilih tindakan yang harus diambil oleh seorang juruteknik jika kandungan haram ditemui pada cakera keras komputer pelanggan.
- I. Contact a first responder.
Hubungi responden pertama.
- II. Confront the customer immediately.
Hadapi pelanggan dengan segera.
- III. Remove and destroy the hard drive.
Keluarkan dan musnahkan cakera keras.
- IV. Document as much information as possible.
Dokumen seberapa banyak maklumat yang mungkin.

CLO1
C4

29.

- A. I and II
- B. I and IV
- C. II and III
- D. III and IV

```
<output ommited>
<server address='192.168.1.2' />
<server port='8752' />
<server protocol='tcp' />
<server protocol='utp' />

<user username="johndoe" password="s3cr3t" roles="administrator"
/>
<user username="jonedoe" password="IP455W0d!" roles="user" />
<user username="guest" password="G355_1T" roles="none" />
<output ommited>
```

Figure A29 / Rajah A29

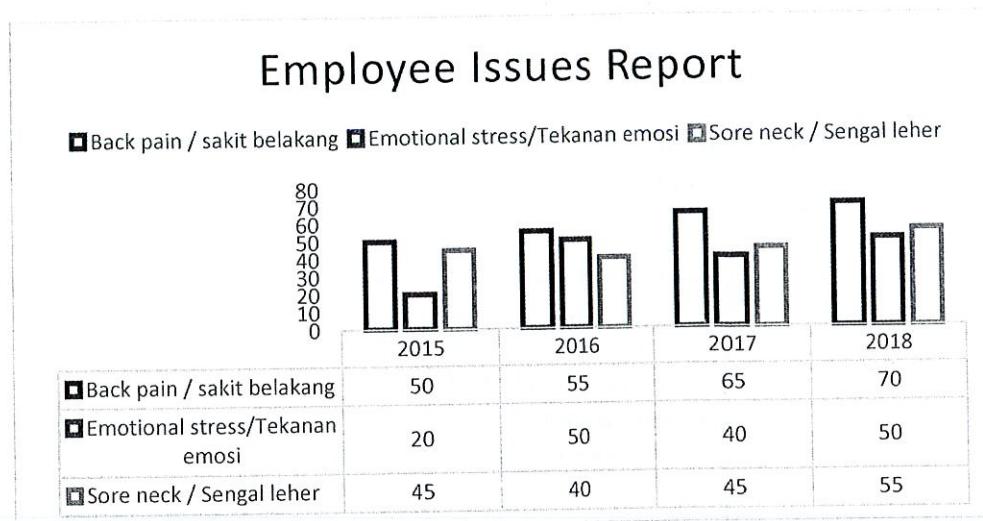
Referring to **Figure A29**, during the troubleshooting of software that is installed on a computer system, a level one technician requires help from a level two technician. The file shown must be sent to the level two technician. Analyze how the level one technician deliver this file.

*Merujuk kepada **Rajah A29**, semasa menyelesaikan masalah perisian yang dipasang pada sistem komputer, juruteknik peringkat satu memerlukan bantuan daripada juruteknik peringkat dua. Fail yang ditunjukkan dalam pameran mesti dihantar ke juruteknik dua tingkat. Analisa bagaimana juruteknik tahap satu menyampaikan fail ini.*

- A. Send the file as it is to the level two technician.
Hantar fail sedia ada kepada juruteknik peringkat dua.
- B. Deliver the file in printed format only.
Menyampaikan fail dalam format bercetak sahaja.
- C. This file should not be shared with the level two technician.
Fail ini tidak boleh dikongsi dengan juruteknik peringkat dua.
- D. Replace all passwords in the file before emailing the file.
Ganti semua kata laluan dalam fail sebelum menghantar e-mel kepada fail.

CLO1
C4

30.

**Figure A30 / Rajah A30**

As a company manager, analyze the main issues complained by your staffs based on **Figure A30**. Classify the action that should be taken to solve the issues.

*Sebagai pengurus syarikat, analisa isu utama yang diadukan oleh staf anda berdasarkan **Rajah A30**. Klasifikasikan tindakan yang perlu diambil bagi menyelesaikan isu ini.*

- A. Change staff workstation with the latest one.
Tukar stesen kerja staf dengan yang terbaru.
- B. Send the report to the board of directors.
Hantar laporan tersebut kepada lembaga pengarah.
- C. Organize a family day to manage staff stress.
Anjurkan hari keluarga untuk menguruskan tekanan staf
- D. Change staff chairs that are suitable for their height.
Gantikan kerusi staf yang bersesuaian mengikut ketinggian.

SECTION B : 55 MARKS***BAHAGIAN B : 55 MARKAH*****INSTRUCTION:**

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

ARAHAN :

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

QUESTION 1***SOALAN 1***

- CLO1 (a) List out **THREE (3)** goal of security in network.

*Senaraikan **TIGA (3)** matlamat keselamatan dalam rangkaian.*

[3 Marks]

[3 Markah]

- CLO1 (b) Explain the types of attack to computer security as below.

Terangkan jenis serangan terhadap keselamatan komputer seperti di bawah.

- (i) Physical

Fizikal

[1 Mark]

[1 Markah]

- (ii) Data

Data

[1 Mark]

[1 Markah]

CLO1	(c)	Define Security Policy. <i>Takrifkan Polisi Keselamatan.</i>	[2 Marks] <i>[2 Markah]</i>
CLO1	(d)	Explain the effect if the security policy is NOT applied in an organization. <i>Terangkan kesan jika polisi keselamatan TIDAK diaplikasikan di dalam sesebuah organisasi.</i>	[2 Marks] <i>[2 Markah]</i>
CLO1	(e)	Explain the application of best practice for managing user account. <i>Terangkan aplikasi amalan terbaik untuk menguruskan akaun pengguna.</i>	[2 Marks] <i>[2 Markah]</i>
CLO2	(f)	Define the purpose of data protection to keep confidential of information. <i>Takrifkan tujuan perlindungan data untuk memastikan kerahsiaan maklumat.</i>	[2 Marks] <i>[2 Markah]</i>

CLO2	(g)	Explain Software License. <i>Terangkan Lesen Perisian.</i>	[2 Marks] <i>[2 Markah]</i>
CLO2	(h)	One of security policies is to set permission for file and folder. Explain the reasons why users should set the adjustment. <i>Salah satu daripada polisi keselamatan ialah untuk menetapkan kebenaran fail dan folder. Terangkan sebab mengapa pengguna perlu membuat penetapan tersebut.</i>	[2 Marks] <i>[2 Markah]</i>
CLO1	(i)	Explain TWO (2) reason why technicians have to manage time and stress properly. <i>Terangkan DUA (2) sebab mengapa juruteknik perlu mengurus masa dan tekanan dengan baik.</i>	[2 Marks] <i>[2 Markah]</i>

- CLO1 (j) Write the process that has to be followed before putting a customer on hold in a phone conversation by completing **Table B1(j)** below.

Tulis proses yang perlu diikuti sebelum meletakkan pelanggan dalam keadaan menunggu ketika pertaulan telefon dengan melengkapkan Jadual B1 (j) dibawah.

Table B1(j) : Process to put customer on hold

Jadual B1(j) : Proses untuk meletakkan pelanggan ketika menunggu

Process to put customer on hold	
<i>Proses untuk meletakkan pelanggan ketika menunggu</i>	
<i>Do / Boleh</i>	<i>Do not / Tidak boleh</i>

[6 Marks]

[6 Markah]

- CLO1 (k) A technician is troubleshooting a computer security issue. The computer was compromised by an attacker as a result of the user having a weak password.

List **THREE (3)** actions that should be taken by the technician take as a preventive measure against this type of attack happening in the future.

*Seorang juruteknik telah menyelesaikan masalah isu keselamatan komputer. Komputer itu telah dijejaskan oleh penyerang kerana pengguna menggunakan kata laluan yang lemah. Senaraikan **TIGA (3)** tindakan yang perlu diambil oleh juruteknik untuk mencegah serangan daripada terjadi di masa hadapan.*

[3 Marks]

[3 Markah]

QUESTION 2**SOALAN 2**

- CLO1 (a) Compare between this two wireless security mode below in terms of security.
Bandingkan antara dua jenis mod keselamatan tanpa wayar dibawah dalam terma keselamatan.
- Wireless Protected Access (WPA)
 - Wireless Equivalent Privacy (WEP)
- [3 Marks]
[3 Markah]
- CLO1 (b) Draw Asymmetric Key Encryption diagram.
Lukis diagram Asymmetric Key Encryption.
- [5 Marks]
[5 Markah]
- CLO2 (c) List **TWO (2)** weaknesses of system without security encryption.
Senaraikan DUA (2) kelemahan pada sistem yang tidak mempunyai penyulitan keselamatan.
- [2 Marks]
[2 Markah]
- CLO2 (d) Explain **TWO (2)** features of Mac Address Filtering.
Jelaskan DUA (2) ciri-ciri Penapisan Mac Address.
- [2 Marks]
[2 Markah]

- CLO2 (e) Ajarfoodie Cafe install a Wi-Fi in their shop for staff use only. The cafe owner finds out an unauthorized person to use their Wi-Fi without a permission. Explain **TWO (2)** solutions he should take in preventing unauthorized person to use their Wi-Fi.

Kafe Ajarfoodie telah memasang Wi-Fi di kedai mereka untuk kegunaan staff sahaja. Pemilik kedai mendapati terdapat pengguna yang tidak sah menggunakan Wi-Fi mereka tanpa kebenaran. Terangkan DUA (2) penyelesaian kepada pemilik untuk menghalang pengguna tidak sah menggunakan Wi-Fi.

[4 Marks]

[4 Markah]

- CLO1 (f) Write **FOUR (4)** troubleshooting processes for security.

Tulis EMPAT (4) proses penyelesaian masalah untuk keselamatan.

[4 Marks]

[4 Markah]

- CLO1 (g) File system renamed, application crash, files dissapeared or files permission has changed eventhough a computer has installed the antivirus. Analyze by explaining **TWO (2)** possible causes for this situation.

Sistem fail dinamakan semula, kerosakan aplikasi, fail hilang atau kebenaran fail telah berubah walaupun komputer telah memasang antivirus. Analisia dengan menerangkan DUA (2) kemungkinan penyebab keadaan ini.

[3 Marks]

[3 Markah]

- CLO2 (h) A computer with the Windows 7 operating system fails to boot when the system is powered on. The technician suspects that the operating system has been attacked by a virus that rendered the system inoperable. Explain **TWO (2)** solutions that can be taken to restore the system functionality.

*Komputer dengan sistem operasi Windows 7 tidak dapat boot apabila sistem diaktifkan. Juruteknik itu mengesyaki bahawa sistem operasi telah diserang oleh virus yang menyebabkan sistem tidak dapat berfungsi. Terangkan **DUA (2)** penyelesaian yang boleh diambil untuk memulihkan fungsi sistem.*

[4 Marks]

[4 Markah]

SOALAN TAMAT