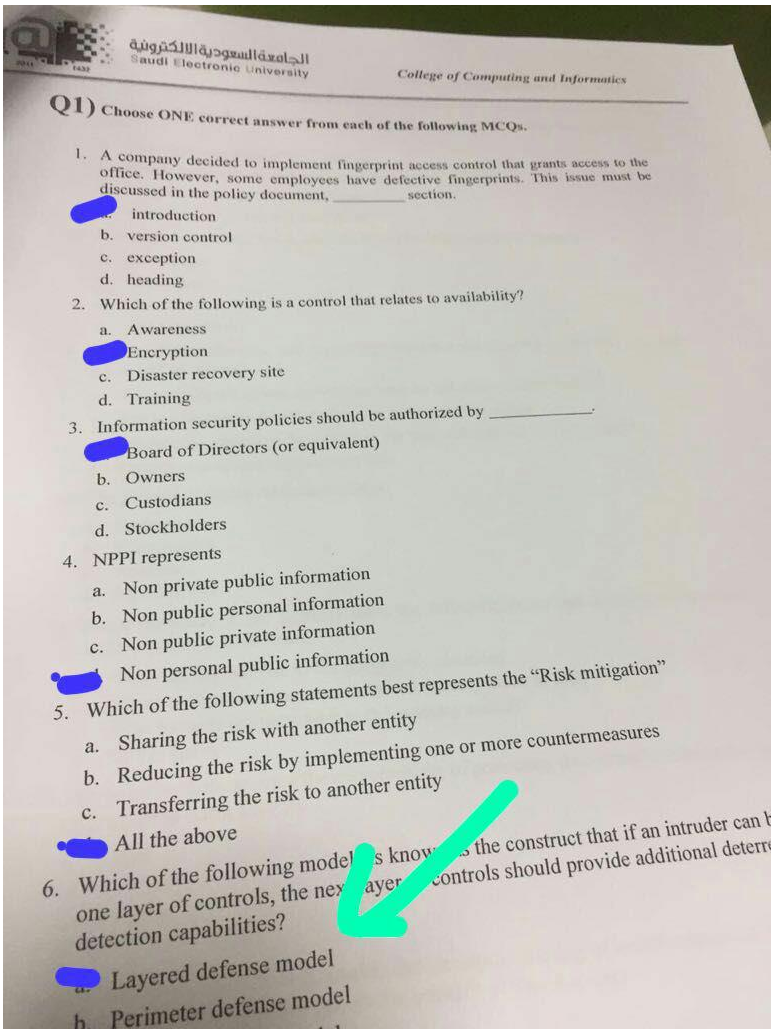
Q2) **For each question, circle True (T) or False (F) as appropriate.**

1.	Using a plain language techniques when writing a policy will make a huge contribution to helping users understand the policy.	T	F
2.	Integrity is the loss of processing capabilities due to natural disaster or human error.	T	F
3.	Maintaining the information systems inventory is the responsibility of the information security officer.	T	F
4.	User accounts and group memberships are created during on board phase.	T	F
5.	Metadata is the data types includes details about a file or document	T	F
6.	Enclave type of network requires a higher degree of protection.	T	F
7.	Evidence needs not to be retained until all legal actions have been completed. Legal action could be civil, criminal, regulatory, or personnel related.	T	F
8.	A cold site is a backup facility that has power, HVAC, and secure access. It has no staged equipment.	T	F
9.	Getting license from SAMA is mandatory to conduct reinsurance activity.	T	F
10.	PCI compliance is a governmental regulation requirement.	T	F

[10 Marks]



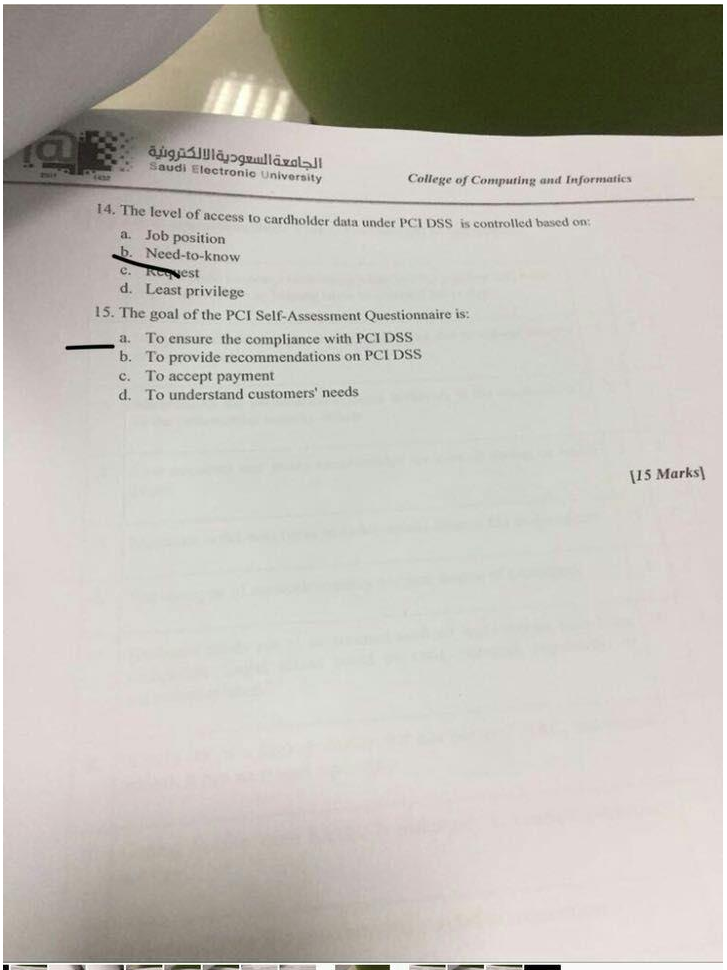
الجامعة السعودية الإلكترونية
Saudi Electronic University

College of Computing and Informatics

Q1) Choose ONE correct answer from each of the following MCQs.

1. A company decided to implement fingerprint access control that grants access to the office. However, some employees have defective fingerprints. This issue must be discussed in the policy document, _____ section.
   a. introduction
   b. version control
   c. exception
   d. heading
2. Which of the following is a control that relates to availability?
   a. Awareness
   b. Encryption
   c. Disaster recovery site
   d. Training
3. Information security policies should be authorized by _____.
   a. Board of Directors (or equivalent)
   b. Owners
   c. Custodians
   d. Stockholders
4. NPPI represents
   a. Non private public information
   b. Non public personal information
   c. Non public private information
   d. Non personal public information
5. Which of the following statements best represents the "Risk mitigation"
   a. Sharing the risk with another entity
   b. Reducing the risk by implementing one or more countermeasures
   c. Transferring the risk to another entity
   d. All the above
6. Which of the following model is known as the construct that if an intruder can b one layer of controls, the next layer of controls should provide additional deterre detection capabilities?
   a. Layered defense model
   b. Perimeter defense model

7. What two factors determine the format of standard operating procedure that should be used?
   a. Cost and complexity of the procedure
   b. [redacted]umber of decisions and number of steps
   c. Language and age of the work force
   d. Number of decisions and exceptions
8. Which type of identity verification the One Time Passcode (OTP) belongs?
   a. Knowledge
   b. [redacted]ssession
   c. Inherence
   d. All of the above
9. Which of the following statements best describes the difference between a security patch and an update?
   a. Patches provide enhancements; updates fix security vulnerabilities.
   b. Patches should be tested; updates do not need to be tested.
   c. Patches fix security vulnerabilities; updates add features and functionality.
   d. Patches cost money; updates are free.
10. The process of digital forensic includes.
   a. Collection
   b. Examination
   c. Analysis
   d. [redacted]ll of Above
11. Threat modeling in the industry takes the following factor into account for business continuity threat assessment
   a. What can happen due to the geographic location?
   b. What could cause processes or information systems to fail?
   c. What hazards are particular to the industry sector?
   d. All the above
12. Financial institutions have the responsibility of protecting their client's information and privacy from harm such as
   a. Fraud
   b. ID Theft
   c. a and b
   d. none of the above
13. Who delivers capabilities to enable the electronic sharing of health related informa[redacted]nd health related services across the country of Saudi Arabia
   a. MOH
   b. Saudi health information exchange privacy and security officer
   c. Saudi Health Information Exchange

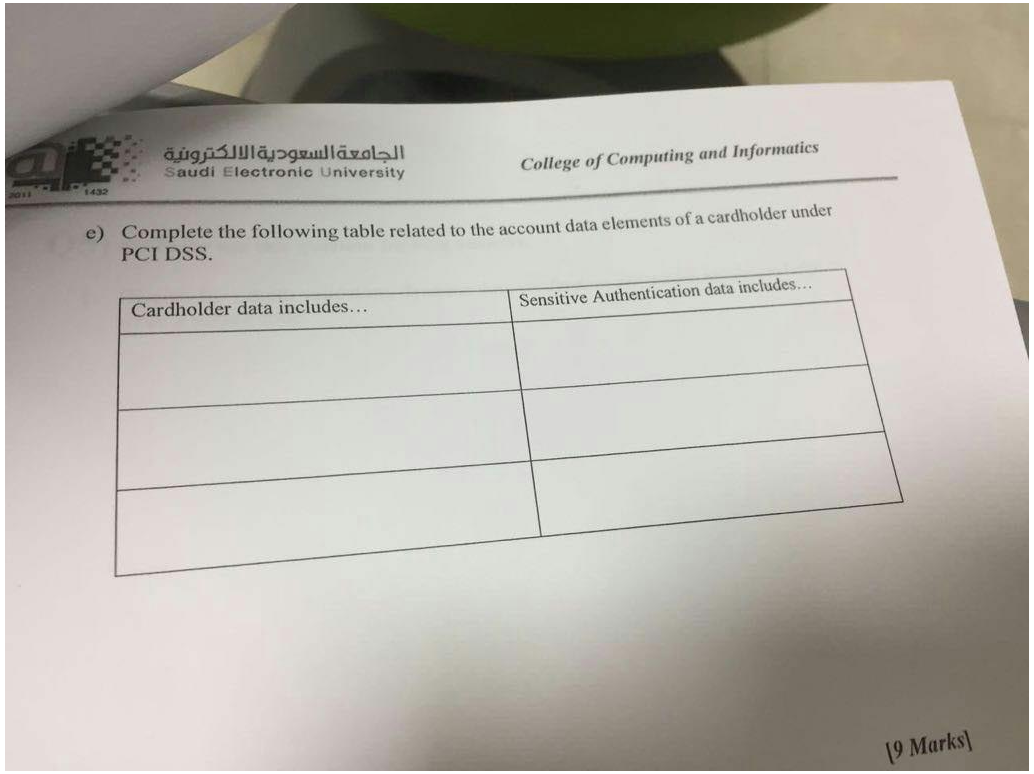


الجامعة السعودية الالكترونية
Saudi Electronic University

College of Computing and Informatics

14. The level of access to cardholder data under PCI DSS is controlled based on:
    a. Job position
    b. Need-to-know
    c. Request
    d. Least privilege
15. The goal of the PCI Self-Assessment Questionnaire is:
    a. To ensure the compliance with PCI DSS
    b. To provide recommendations on PCI DSS
    c. To accept payment
    d. To understand customers' needs

\15 Marks



الجامعة السعودية الالكترونية
Saudi Electronic University

College of Computing and Informatics

e) Complete the following table related to the account data elements of a cardholder under PCI DSS.

Cardholder data includes…	Sensitive Authentication data includes…

[9 Marks]

Fill-in each blank with the most suitable word from the table.

incident response plan	policies	footprinting	information asset	plans
questionnaire	tabletop exercises	authentication	multi-factor authentication	card holder data
information system	PKI	procedures	fingerprinting	audit

1. If _____ are not relevant, they will be ignored or, worse, dismissed as unnecessary and management will be perceived as being out of touch.
2. _____ are strategic and tactical guidance used to execute an initiative or respond to a situation, within a certain timeframe, usually with defined stages and with designated resources.
3. A definable piece of information that adds value to the organizations is known as _____.
4. A job interview is a perfect _____ opportunity for hackers and social engineers.
5. _____ is the framework and services used to create, distribute, manage, and revoke public keys.
6. An _____ is a roadmap of reporting, responding, and recovery actions.
7. _____ can be conducted as structured reviews or simulations.
8. The self-assessment of security framework of an organization is performed using _____.
9. Remote access to HIE requires _____.
10. Under PCI DSS, Primary Account Number (PAN) is an example of _____.

\10 Mar

Q1) Choose ONE correct answer from each of the following MCQs.

1. A company decided to implement fingerprint access control that grants access to the office. However, some employees have defective fingerprints. This issue must be discussed in the policy document, _____ section.
   a. introduction
   b. version control
   c. exception
   d. heading
2. Which of the following is a control that relates to availability?
   a. Awareness
   b. Encryption
   c. Disaster recovery site
   d. Training
3. Information security policies should be authorized by _____.
   a. Board of Directors (or equivalent)
   b. Owners
   c. Custodians
   d. Stockholders
4. NPPI represents
   a. Non private public information
   b. Non public personal information
   c. Non public private information
   d. Non personal public information
5. Which of the following statements best represents the "Risk mitigation"
   a. Sharing the risk with another entity
   b. Reducing the risk by implementing one or more countermeasures
   c. Transferring the risk to another entity
   d. All the above
6. Which of the following models is known as the construct that if an intruder can b one layer of controls, the next layer of controls should provide additional deterr detection capabilities?
   a. Layered defense model
   b. Perimeter defense model

7. What two factors determine the format of standard operating procedure that should be used?
   a. Cost and complexity of the procedure
   b. Number of decisions and number of steps
   c. Language and age of the work force
   d. Number of decisions and exceptions
8. Which type of identity verification the One Time Passcode (OTP) belongs?
   a. Knowledge
   b. Possession
   c. Inherence
   d. All of the above
9. Which of the following statements best describes the difference between a security patch and an update?
   a. Patches provide enhancements; updates fix security vulnerabilities.
   b. Patches should be tested; updates do not need to be tested.
   c. Patches fix security vulnerabilities; updates add features and functionality.
   d. Patches cost money; updates are free.
10. The process of digital forensic includes.
   a. Collection
   b. Examination
   c. Analysis
   d. All of Above
11. Threat modeling in the industry takes the following factor into account for business continuity threat assessment
   a. What can happen due to the geographic location?
   b. What could cause processes or information systems to fail?
   c. What hazards are particular to the industry sector?
   d. All the above
12. Financial institutions have the responsibility of protecting their client's information and privacy from harm such as
   a. Fraud
   b. ID Theft
   c. a and b
   d. none of the above
13. Who delivers capabilities to enable the electronic sharing of health related informa and health related services across the country of Saudi Arabia
   a. MOH
   b. Saudi health information exchange privacy and security officer
   c. Saudi Health Information Exchange

7. What two factors determine the format of standard operating procedure that should be used?
   a. Cost and complexity of the procedure
   b. Number of decisions and number of steps
   c. Language and age of the work force
   d. Number of decisions and exceptions
8. Which type of identity verification the One Time Passcode (OTP) belongs?
   a. Knowledge
   b. Possession
   c. Inherence
   d. All of the above
9. Which of the following statements best describes the difference between a security patch and an update?
   a. Patches provide enhancements; updates fix security vulnerabilities.
   b. Patches should be tested; updates do not need to be tested.
   c. Patches fix security vulnerabilities; updates add features and functionality.
   d. Patches cost money; updates are free.
10. The process of digital forensic includes.
   a. Collection
   b. Examination
   c. Analysis
   d. All of Above
11. Threat modeling in the industry takes the following factor into account for business continuity threat assessment
   a. What can happen due to the geographic location?
   b. What could cause processes or information systems to fail?
   c. What hazards are particular to the industry sector?
   d. All the above
12. Financial institutions have the responsibility of protecting their client's information and privacy from harm such as
   a. Fraud
   b. ID Theft
   c. a and b
   d. none of the above
13. Who delivers capabilities to enable the electronic sharing of health related informa and health related services across the country of Saudi Arabia
   a. MOH
   b. Saudi health information exchange privacy and security officer
   c. Saudi Health Information Exchange

Q1) Choose ONE correct answer from each of the following MCQs.

1. A company decided to implement fingerprint access control that grants access to the office. However, some employees have defective fingerprints. This issue must be discussed in the policy document, _____ section.
   a. introduction
   b. version control
   c. exception
   d. heading
2. Which of the following is a control that relates to availability?
   a. Awareness
   b. Encryption
   c. Disaster recovery site
   d. Training
3. Information security policies should be authorized by _____.
   a. Board of Directors (or equivalent)
   b. Owners
   c. Custodians
   d. Stockholders
4. NPPI represents
   a. Non private public information
   b. Non public personal information
   c. Non public private information
   d. Non personal public information
5. Which of the following statements best represents the "Risk mitigation"
   a. Sharing the risk with another entity
   b. Reducing the risk by implementing one or more countermeasures
   c. Transferring the risk to another entity
   d. All the above
6. Which of the following models is known as the construct that if an intruder can b one layer of controls, the next layer of controls should provide additional deterr detection capabilities?
   a. Layered defense model
   b. Perimeter defense model

Q2) For each question, circle True (T) or False (F) as appropriate.

1.	Using a plain language techniques when writing a policy will make a huge contribution to helping users understand the policy.	T	F
2.	Integrity is the loss of processing capabilities due to natural disaster or human error.	T	F
3.	Maintaining the information systems inventory is the responsibility of the information security officer.	T	F
4.	User accounts and group memberships are created during on board phase.	T	F
5.	Metadata is the data types includes details about a file or document.	T	F
6.	Enclave type of network requires a higher degree of protection.	T	F
7.	Evidence needs not to be retained until all legal actions have been completed. Legal action could be civil, criminal, regulatory, or personnel related.	T	F
8.	A cold site is a backup facility that has power, HVAC, and secure access. It has no staged equipment.	T	F
9.	Getting license from SAMA is mandatory to conduct reinsurance activity.	T	F
10.	PCI compliance is a governmental regulation requirement.	T	F

{10 Marks}

Fill-in each blank with the most suitable word from the table.

incident response plan	policies	footprinting	information asset	plans
questionnaire	tabletop exercises	authentication	multi-factor authentication	card holder data
information system	PKI	procedures	fingerprinting	audit

1. If _____ are not relevant, they will be ignored or, worse, dismissed as unnecessary and management will be perceived as being out of touch.
2. _____ are strategic and tactical guidance used to execute an initiative or respond to a situation, within a certain timeframe, usually with defined stages and with designated resources.
3. A definable piece of information that adds value to the organizations is known as _____.
4. A job interview is a perfect _____ opportunity for hackers and social engineers.
5. _____ is the framework and services used to create, distribute, manage, and revoke public keys.
6. An _____ is a roadmap of reporting, responding, and recovery actions.
7. _____ can be conducted as structured reviews or simulations.
8. The self-assessment of security framework of an organization is performed using _____.
9. Remote access to HIE requires _____.
10. Under PCI DSS, Primary Account Number (PAN) is an example o _____.

\10 Mar

Q4) Answer the following questions briefly.

a) List and describe five different types of malware.

\7.5 Mark

b) What is the purpose of Whitelisting/Blacklisting?

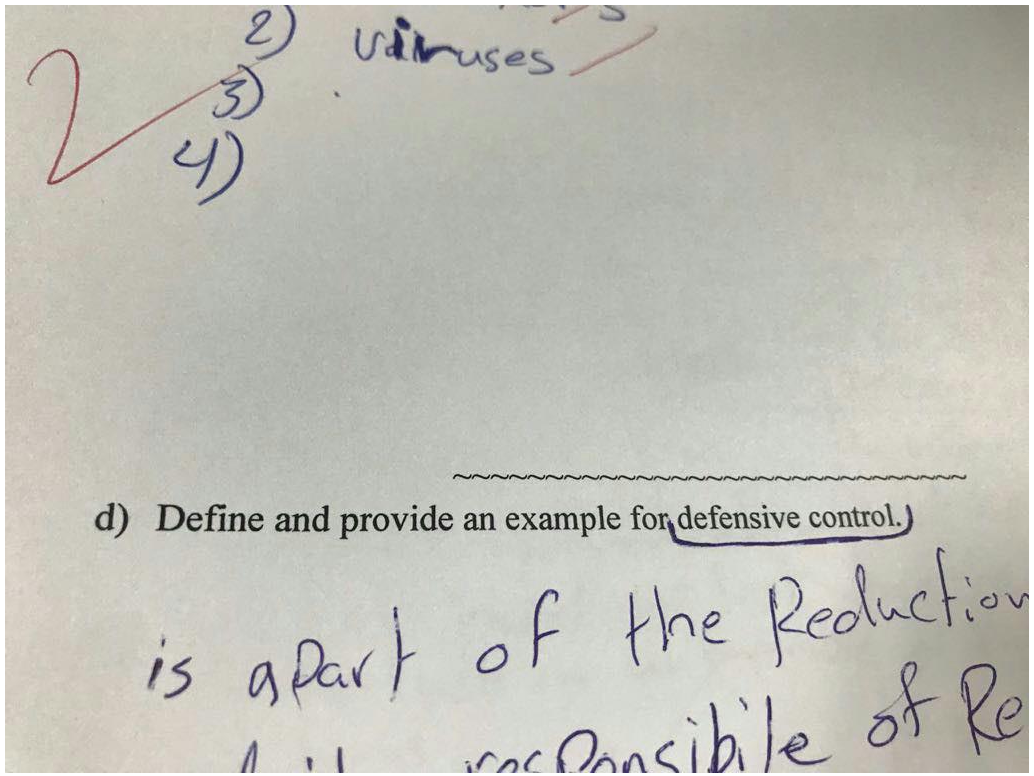
Q1) Choose ONE correct answer from each of the following MCQs.

1. A company decided to implement fingerprint access control that grants access to the office. However, some employees have defective fingerprints. This issue must be discussed in the policy document, _____ section.
   a. introduction
   b. version control
   c. exception
   d. heading
2. Which of the following is a control that relates to availability?
   a. Awareness
   b. Encryption
   c. Disaster recovery site
   d. Training
3. Information security policies should be authorized by _____.
   a. Board of Directors (or equivalent)
   b. Owners
   c. Custodians
   d. Stockholders
4. NPPI represents
   a. Non private public information
   b. Non public personal information
   c. Non public private information
   d. Non personal public information
5. Which of the following statements best represents the "Risk mitigation"
   a. Sharing the risk with another entity
   b. Reducing the risk by implementing one or more countermeasures
   c. Transferring the risk to another entity
   d. All the above
6. Which of the following models is known as the construct that if an intruder can b one layer of controls, the next layer of controls should provide additional deterr detection capabilities?
   a. Layered defense model
   b. Perimeter defense model

c) List all factors that are considered during the Business Continuity Threat Assessment.

[6 *Marks*]

d) Who enforces and monitors the Heath Information Exchange (HIE) policies? List any three users of HIE policies.


2)
viruses
3)
4)
d) Define and provide an example for defensive control.
is apart of the Reduction
responsibile of Re

Q5) You may use this question for long answers.

a) Compare different employee agreements.

Sl.No	Confidentiality agreement	Acceptable use agreement
Definition	agreemat assigned by the employee ~~that~~ about the informations of the company and its value and it must show the enforcemnts and ~~that~~	is the agreemat between the hire and IS section about using ~~the~~ some of the equipments like laptops or others
Goal	to protect the confidintial informat of theaf or lost or use in unfayerable way	to inform the employee that he or she cant use the equipments of the company for personal goals but only for the business needs.
Important in situations	in case of the employee retire or stop working for any reaser and if he take any informations or in case of third party worker in the company	in case of harm of the devices or lost them

tell the ~~IP~~ information thing and access net

or internet access

when employee newly joins

[15 Marks]

Q5) You may use this question for long answers.

1. Discuss how input validation, dynamic data verification and output validation helps to write a secure code.

Q3) Fill-in each blank with the most suitable word from the table.

Service level agreement	Continuity plan	Boards of Directors	Acceptable use agreement	Governance
Operational management	Guideline	background-check	plan	Owners

Owner

1. _____ are often composed of experienced albeit nontechnical business people from a spectrum of industry sectors.
2. The document that is used to direct a user on how to respond to a security event with certain time frame is a Guidline.
3. service level agreement is an agreement between a service provider and a customer that specifically addresses availability of services.
4. _____ Plan is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors.
5. Companies should seek consent from employees before launching Background check

[5*Marks*]

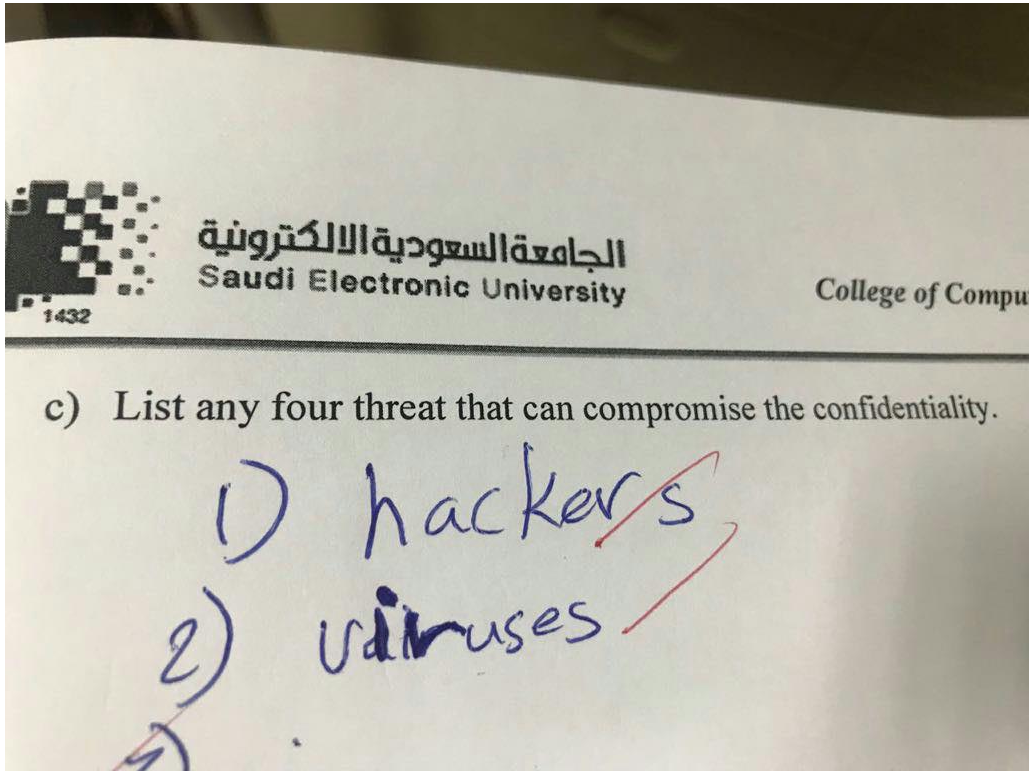
Policy should be documnteel.

14

) Develop an example that shows the following: policy and related standard.

) : - Employees should wear the
the company at
time

uld be an emp
wh


الجامعة السعودية الالكترونية
Saudi Electronic University
1432
College of Compu
c) List any four threat that can compromise the confidentiality.
1) hackers
2) viruses

7. Which of the following is not the responsibility of information owner?
   a. Defining asset
   b. Implementing security controls
   c. Assigning value to the asset
   d. Deciding who should have the access to the asset

8. Which of the following national security classifications requires the least protection?
   a. Secret
   b. Unclassified
   c. Top Secret
   d. Confidential

9. Which of the following terms best describes an example of a hardware asset?
   a. Servers
   b. Firewalls
   c. Operating system
   d. Applications

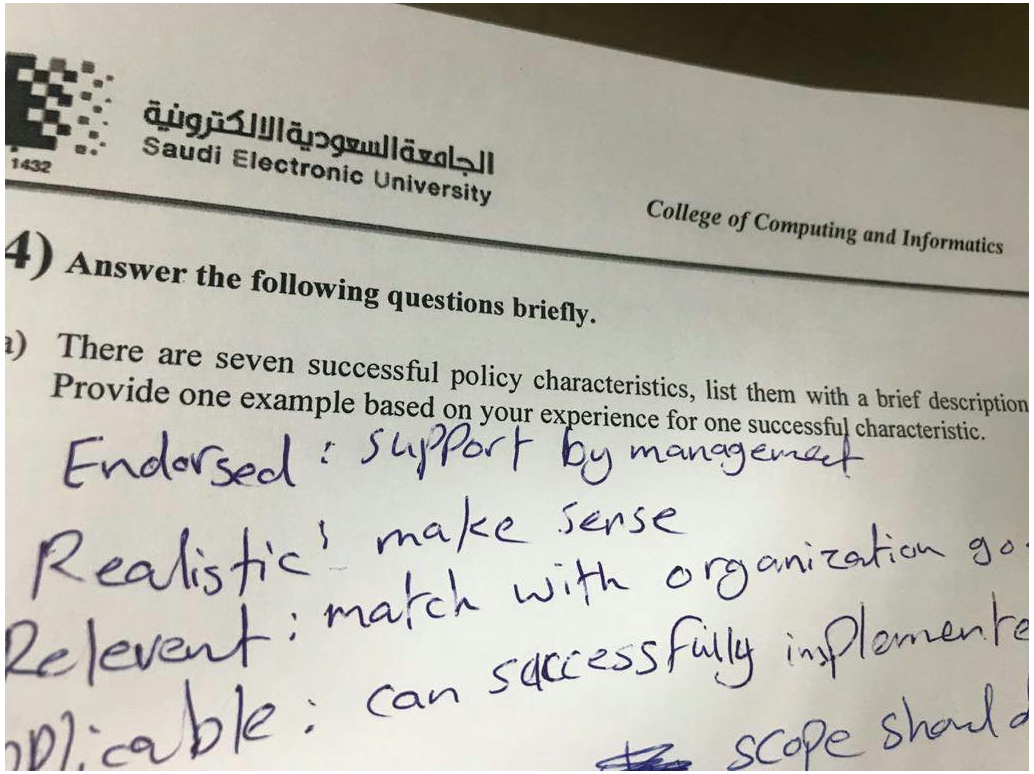
10. Password management, internet access, handling standards are explained in
   a. Confidentiality agreement
   b. Acceptable use agreement
   c. Third party agreement
   d. Vendor policy agreement

[*10 Marks*]

Q2) For each question, circle True (T) or False (F) as appropriate.

1.	The policy lifecycle spans four phases: planning, analysis, design, and implementation.	T	(F)
2.	Policy definitions aim to enhance employee understanding of policies and rules.	(T)	F
3.	Objective of confidentiality is protection from unauthorized access.	(T)	F
4.	An annual review of the information security policy must be conducted.	(T)	F
5.	According to SETA model, Awareness is training.	T	(F)

[5Ma


الجامعة السعودية الإلكترونية
Saudi Electronic University
1432
College of Computing and Informatics
4) Answer the following questions briefly.
a) There are seven successful policy characteristics, list them with a brief description
Provide one example based on your experience for one successful characteristic.
Endorsed : support by management
Realistic : make sense
Relevent : match with organization go
Applicable : can successfully implemente
scope shoul

Q2) For each question, circle True (T) or False (F) as appropriate.

1.	Using a plain language techniques when writing a policy will make a huge contribution to helping users understand the policy.	T	F
2.	Integrity is the loss of processing capabilities due to natural disaster or human error.	T	F
3.	Maintaining the information systems inventory is the responsibility of the information security officer.	T	F
4.	User accounts and group memberships are created during on board phase.	T	F
5.	Metadata is the data types includes details about a file or document.	T	F
6.	Enclave type of network requires a higher degree of protection.	T	F
7.	Evidence needs not to be retained until all legal actions have been completed. Legal action could be civil, criminal, regulatory, or personnel related.	T	F
8.	A cold site is a backup facility that has power, HVAC, and secure access. It has no staged equipment.	T	F
9.	Getting license from SAMA is mandatory to conduct reinsurance activity.	T	F
10.	PCI compliance is a governmental regulation requirement.	T	F

[10 Marks]

Fill in each blank with the most suitable word from the table.

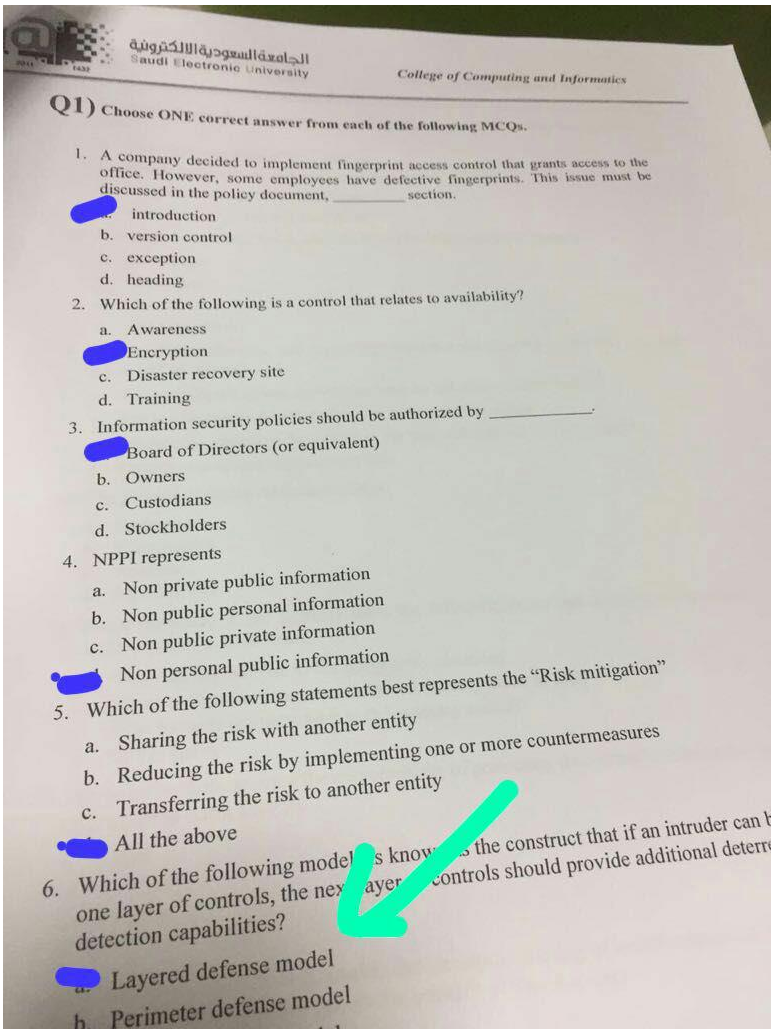
incident response plan 6	policies 1	footprinting 4	information asset 3	plans 2
questionnaire 8	tabletop exercises	authentication	multi-factor authentication 9	card holder data 10
information system	PKI 5	procedures	fingerprinting	audit 7

1. If _____ are not relevant, they will be ignored or, worse, dismissed as unnecessary and management will be perceived as being out of touch.
2. _____ are strategic and tactical guidance used to execute an initiative or respond to a situation, within a certain timeframe, usually with defined stages and with designated resources.
3. A definable piece of information that adds value to the organizations is known as _____.
4. A job interview is a perfect _____ opportunity for hackers and social engineers.
5. _____ is the framework and services used to create, distribute, manage, and revoke public keys.
6. An _____ is a roadmap of reporting, responding, and recovery actions.
7. _____ can be conducted as structured reviews or simulations.
8. The self-assessment of security framework of an organization is performed using _____.
9. Remote access to HIE requires _____.
10. Under PCI DSS, Primary Account Number (PAN) is an example o _____.

\10 Mar

Q1) Choose ONE correct answer from each of the following MCQs.

1. "Approve written information security policies" is responsibilities of:
   a. Internal Auditor
   b. Board of Directors
   c. Foreign officer
   d. All of Above
2. To claim a forgotten password, click on the "forgot password" button. Then, enter your user ID. Answer the security questions. If successful, a new password page will pop up; then, you can change the password safely. The above scenario best describes
   a. Baseline
   b. Procedure
   c. Standard
   d. Guidelines
3. Which of the following terms best describes the granting of users and systems a predetermined level of access to information resources?
   a. Authorization
   b. Accountability
   c. Availability
   d. Assurance
4. Which of the following statements best describes independence in the context of auditing?
   a. The auditor is not an employee of the company
   b. The auditor is certified to conduct audits
   c. The auditor is not responsible for, benefited from, or in any way influenced by the audit outcome
   d. Each auditor presents his or her own opinion
5. Which of the following factors that influence the information security decision making and policy development
   a. Risks related to achieving their business objectives.
   b. Regulatory Requirements
   c. Guiding principles
   d. Above All
6. The process of describing the upgrading or changing the classification levels is termed as
   a. Classification
   b. Declassification
   c. Negative classification
   d. Reclassification



الجامعة السعودية الإلكترونية
Saudi Electronic University

College of Computing and Informatics

Q1) Choose ONE correct answer from each of the following MCQs.

1. A company decided to implement fingerprint access control that grants access to the office. However, some employees have defective fingerprints. This issue must be discussed in the policy document, _____ section.
   a. introduction
   b. version control
   c. exception
   d. heading
2. Which of the following is a control that relates to availability?
   a. Awareness
   b. Encryption
   c. Disaster recovery site
   d. Training
3. Information security policies should be authorized by _____.
   a. Board of Directors (or equivalent)
   b. Owners
   c. Custodians
   d. Stockholders
4. NPPI represents
   a. Non private public information
   b. Non public personal information
   c. Non public private information
   d. Non personal public information
5. Which of the following statements best represents the "Risk mitigation"
   a. Sharing the risk with another entity
   b. Reducing the risk by implementing one or more countermeasures
   c. Transferring the risk to another entity
   d. All the above
6. Which of the following model is known as the construct that if an intruder can b one layer of controls, the next layer of controls should provide additional deterre detection capabilities?
   a. Layered defense model
   b. Perimeter defense model