EXTERNAL INTEGRATED SUMMATIVE ASSESSMENT

Theory

STUDENT NAME & SURNAME	
ID NUMBER	
EISA REGISTRATION NUMBER	
ASSESSMENT CENTRE	
ASSESSMENT CENTRE ACCREDITATION NUMBER	
QUALIFICATION	
SAQA ID	
CREDITS	
PAPER	
DATE OF EISA	
DURATION	2 Hours
TOTAL MARKS	100

Theory Assessment (100 Marks)

Question 1: Multiple Choice Questions (20 Marks)

1. What is the primary goal of cybersecurity?

a) Enhance user interface.

b) Protect data and systems.

c) Improve processing speed.

d) Boost data storage.

2. Which law regulates data protection in South Africa?

a) GDPR

b) ISO27001

c) POPIA

d) HIPAA

3. Which three principles make up the cybersecurity CIA triad?

a) Confidentiality, Integrity, Availability.

b) Cryptography, Integrity, Authentication.

c) Compliance, Integrity, Availability.

d) Confidentiality, Accountability, Access.

4. What type of malware pretends to be legitimate software?

a) Worm

b) Ransomware

c) Spyware

d) Trojan

5. ***Which device is commonly used for input in computing?***

a) Monitor

b) Mouse

c) CPU

d) Speaker

6. ***Which network security device helps filter unauthorised access?***

a) Hard drive

b) Firewall

c) Printer

d) Webcam

7. ***What is SQL mainly used for in cybersecurity?***

a) Encrypting data.

b) Querying databases.

c) Scanning for vulnerabilities.

d) Securing networks.

8. ***Which phase in the Design Thinking process focuses on identifying user needs?***

a) Define

b) Empathise

c) Prototype

d) Test

9. ***What is the focus of the Fourth Industrial Revolution (4IR)?***

a) Manufacturing.

b) Digital technology and AI.

c) Printing press.

d) Telephone networks.

10. In logical thinking, what is a binary number?

a) A decimal number.

b) A number represented by 1s and 0s.

c) A negative number.

d) A hexadecimal number.

11. Which type of attack involves tricking individuals into revealing confidential information?

a) Phishing.

b) Denial-of-Service.

c) SQL Injection.

d) Malware Infection.

12. Which of the following is a common feature of a secure password?

a) Repeating characters.

b) All lowercase letters.

c) A mix of letters, numbers, and symbols.

d) Simple and easy to remember.

13. What does GDPR stand for in data protection?

a) General Data Policy Regulations.

b) Government Data Privacy Requirements.

c) General Data Protection Regulation.

d) General Database Protection Rules.

14. What kind of device is used to store data long-term?

a) RAM

b) CPU

c) SSD

d) Cache

15. Which of the following best describes a vulnerability?

a) A new feature added to the software.

b) A weakness that can be exploited.

c) A program that performs regular updates.

d) A user's password.

16. Which concept in cybersecurity ensures that information is accessible only to those with permission?

a) Integrity

b) Availability

c) Confidentiality

d) Authentication

17. Which of the following is a key benefit of multi-factor authentication (MFA)?

a) Easier login for all users

b) Reduces network traffic

c) Provides an extra layer of security

d) Automatically updates passwords

18. What does "DoS" stand for in cybersecurity?

a) Denial-of-Security

b) Denial-of-Service

c) Defense-of-Systems

d) Disruption-of-Service

19. Which of the following is a method used to prevent unauthorised access to data in transit?

a) Encryption

b) Compression

c) Sorting

d) Caching

20. What is a key aspect of the Design Thinking process?

a) Directly testing solutions on users.

b) Ignoring user feedback

c) Prioritising speed over accuracy

d) Focusing on understanding user needs

Question 2: Short Answer Questions (20 Marks)

1. ***Explain two main purposes of a firewall in cybersecurity. (2 marks)***

2. ***What is identity theft, and why is it harmful? (2 marks)***

3. ***Describe two key principles of cybersecurity ethics. (2 marks)***

4. ***Why is data encryption important in data security? (2 marks)***

5. ***What is the primary role of design thinking in innovation? (2 marks)***

6. ***List two components essential for computer processing. (2 marks)***

7. ***Identify two ways the Fourth Industrial Revolution is changing the workplace. (2 marks)***

8. ***What is a network vulnerability? Give an Assessmentple. (2 marks)***

9. ***Explain the process of 'reconnaissance' in a cyber threat context. (2 marks)***

10. ***Why is binary logic essential for cybersecurity professionals? (2 marks)***

Question 3: True/False (20 Marks)

1. **True or False:**

The goal of a Denial-of-Service (DoS) attack is to make a system or network unavailable to its intended users.

2. **True or False:**

Only public networks, such as Wi-Fi in cafes, are vulnerable to cyber-attacks.

3. **True or False:**

Data encryption protects information by converting it into code, making it unreadable to unauthorised users.

4. **True or False:**

Ransomware encrypts files on the victim's device and demands payment for decryption.

5. **True or False:**

Data masking is used to display sensitive data in its original form but only to authorised users.

6. **True or False:**

Public key encryption uses two keys—a public key for encryption and a private key for decryption.

7. **True or False:**

Anti-virus software is designed to protect against all forms of cyber threats, including social engineering.

8. **True or False:**

Ethical hacking is conducted by cybersecurity professionals to identify weaknesses in systems before malicious hackers exploit them.

9. **True or False:**

The term "malware" includes viruses, worms, ransomware, and spyware.

10. **True or False:**

Cloud storage eliminates the need for regular data backup.

11. **True or False:**

Firewalls can be configured to block both incoming and outgoing traffic based on specific rules.

12. **True or False:**

The principle of least privilege ensures that users have only the access necessary to perform their jobs.

13. **True or False:**

Social engineering relies on manipulating human behaviour rather than exploiting technical vulnerabilities to gain unauthorised access.

14. **True or False:**

Data encryption only protects data at rest, not data in transit.

15. **True or False:**

An Intrusion Prevention System (IPS) can both detect and block potential threats in real-time.

16. **True or False:**

Zero-day vulnerabilities are security flaws that have been publicly disclosed and patched.

17. **True or False:**

Social engineering attacks exploit human behaviour rather than technical vulnerabilities.

18. **True or False:**

The Fourth Industrial Revolution focuses mainly on advances in manufacturing processes.

19. **True or False:**

Public Wi-Fi networks are generally safe to use without additional security measures.

20. **True or False:**

Antivirus software can detect and remove all forms of malware, including previously unknown threats.

Question 3: Scenario-Based Questions (40 Marks)

Scenario 1: Email Phishing Detection (4 Marks)

You receive an email from a source/sender that appears to be your bank, requesting you to verify your account details by clicking a link.

1. ***What type of attack does this represent? (1 mark)***

2. ***What are two indicators that could help you identify this type of cyber-attack attempt? (2 marks)***

3. ***Describe one safe action you should take upon receiving this email. (1 mark)***

Scenario 2: Data Breach Response (4 Marks)

Your company experiences a data breach, potentially compromising customer information.

1. ***Identify two immediate actions your company should take. (2 marks)***

2. ***Explain one long-term measure your company can implement to prevent future breaches. (2 marks)***

Scenario 3: Network Security and Threat Detection (8 Marks)

Your company has installed network monitoring tools and has noticed unusual traffic from several IP addresses. You suspect it might be a security threat.

1. ***What initial action would you take to address this potential threat? (4 marks)***

2. ***Describe two ways a firewall or intrusion detection system can help manage this type of threat. (4 marks)***

Scenario 4: Data Privacy Compliance (8 Marks)

An online service is planning to collect detailed personal information from users, including their location and browsing history.

1. ***What are two important legal considerations the company should review before collecting user data? (4 marks)***

2. ***Explain why gaining user consent is crucial when collecting sensitive data. (4 marks)***

Scenario 5: Security Measures for Personal Devices (6 Marks)

An employee is using their personal laptop for work, which includes handling sensitive company data.

1. ***List and describe two cybersecurity practices the employee should follow to protect company data on a personal device. (4 marks)***

2. ***Describe one risk of not following security practices on personal devices. (2 marks)***

Scenario 6: Basics of Logical Problem-Solving (5 Marks)

While Assessmentining security data, you need to calculate the impact of a recent system error that led to inaccurate reporting of user activities.

1. ***Explain how logical problem-solving can help identify the cause of this error. (2 marks)***

2. ***Provide an Assessmentple of a simple calculation or data verification step that could help confirm if the error is resolved. (3 marks)***

Scenario 7: Design Thinking in Cybersecurity (5 Marks)

Your company wants to introduce a new feature for their app that will use AI to detect and respond to cyber threats.

1. ***List two steps in the design thinking process that would help develop this feature effectively. (2 marks)***

2. ***Explain why understanding user needs is critical in designing a cybersecurity feature. (3 marks)***

MICTSETA | Media, Information And Communication Technologies Sector Education And Training Authority

SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES