



THE TECHNICAL UNIVERISTY OF MOMBASA

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
CERTIFICATE IN INFORMATION TECHNOLOGY & MAINTENANCE
(CITM 12S)

EIT 1131: FUNDAMENTALS OF INFORMATION SECURITY

END OF SEMESTER EXAMINATION

SERIES: APRIL 2013

TIME: 2 HOURS

Instructions to Candidates:

You should have the following for this examination

This paper consists of **FIVE** questions. Attempt question **ONE** and any other **TWO** questions

Maximum marks for each part of a question are as shown

This paper consists of **THREE** printed pages

Question One (Compulsory)

- a) Define the following: **(2 marks)**
(i) Security
(ii) Threat
- b) Describe the term attack in relation to computer information security. **(1 mark)**
- c) Differentiate between information security and computer security. **(2 marks)**
- d) Describe the following terms in relation to information security. **(5 marks)**
(i) Confidentiality
(ii) Authentication
(iii) Availability
(iv) Non-repudiation
(v) Integrity
(vi) Bluesnarfing
- e) Discuss the different mechanisms of security information from different threats. **(8 marks)**
- f) Distinguish between data and information. **(2 marks)**

Question Two

- a) Describe the following in relation to computer security threats. **(10 marks)**
(i) Employee sabotage
(ii) Malicious hackers
(iii) Espionage
(iv) Eavesdropping
- b) Discuss security measures that can be taken to mitigate the above security threats. **(10 marks)**

Question Three

- a) Define disaster recovery plan. **(2 marks)**
- b) State and explain **THREE** types of malicious code. **(6 marks)**
- c) State and explain the reasons of performing risk analysis. **(8 marks)**
- d) Describe the term denial of service and its causes. **(4 marks)**

Question Four

- a) Differentiate the following:
(i) Spyware and Trojan horse **(2 marks)**
(ii) Intrusion detection systems and firewall **(4 marks)**
(iii) Encryption and authenticity **(4 marks)**
- b) Discuss different attacks that cause threats to information. **(6 marks)**

c) State and explain the content of security plan. **(4 marks)**

Question Five

a) Discuss various ways of preparing for a disaster. **(4 marks)**

b) Describe the procedure of disaster preparedness. **(8 marks)**

c) Describe the policies of disaster preparedness **(8 marks)**