TECHNICAL UNIVERISTY OF MOMBASA

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

CERTIFICATE IN INFORMATION TECHNOLOGY & MAINTENANCE
(CICM 13M)

EIS 1101: FUNDAMENTALS OF INFORMATION SECURITY

END OF SEMESTER EXAMINATION
SERIES: DECEMBER 2013
TIME: 2 HOURS

Instructions to Candidates:
You should have the following for this examination

- *Answer Booklet*

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 information security **(2 marks)**

b) Differentiate between availability and integrity in relation to information security. **(4 marks)**

c) Discuss different attacks that may cause threats to information system **(6 marks)**

d) Describe the following in relation to information security.
- **(i)** Encryption
- **(ii)** Non-repudiation
- **(iii)** Authenticity
- **(iv)** Confidentiality **(8 marks)**

e) Describe THREE types of malicious code **(6 marks)**

f) Define risk assessment **(2 marks)**

g) State TWO emerging information security challenges **(2 marks)**

Question Two

a) Why is it significance to secure information **(6 marks)**

b) Describe the following measures of information security in computer systems **(8 marks)**
- **(i)** Firewall
- **(ii)** Backup
- **(iii)** Access authorization
- **(iv)** Intrusion detection systems

c) Discuss different recovery measures that may be taken in case of data loss. **(6 marks)**

Question Three

a) State the function of a proxy server **(2 marks)**

b) State and explain TWO physical threats and ways of reducing those threats **(4 marks)**

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

d) State and explain THREE types of network attacks **(10 marks)**

Question Four

a) Define “disaster recovery plan **(2 marks)**

b) State and describe the procedure of performing risk assessment **(8 marks)**

c) Discuss the policies of disaster preparedness **(10 marks)**

Question Five

a) Distinguish between data and information **(2 marks)**

b) State the difference between Trojan horse and spyware and how it causes harm to information. **(4** marks)

c) Differentiate between intrusion detection systems and firewall **(4 marks)**

d) Describe the following in relation to information security. **(10 marks)**

(i) Malicious hackers
(ii) Employee sabotage
(iii) Eavesdropping
(iv) Social engineering
(v) Human error