THE MOMBASA POLYTECHNIC UNIVERSITY COLLEGE

(A Constituent College of JKUAT)

Faculty of Engineering & Technology

DEPARTMENT COMPUTER SCIENCE & INFORMATION TECHNOLOGY

CERTIFICATE IN INFORMATION TECHNOLOGY – CIT 2K 11M

EIT 1131: FUNDAMENTALS OF INFORMATION SECURITY

END OF SEMESTER EXAMINATIONS

SERIES: DECEMBER 2011

TIME: 2 HOURS

Instructions to Candidates:

You should have the following for this examination

- *Answer Booklet*

This paper consist of **FIVE** questions in **TWO** sections **A** & **B**
Answer question **ONE (COMPULSORY)** and any other **TWO** questions
Maximum marks for each part of a question are as shown
This paper consists of **THREE** printed pages

SECTION A (COMPULSORY)

Question 1 - 30 Marks

a) Define security [1mark]
b) Define a threat [1marks]
c) Describe the term "attack' in relation to computer information security [1marks]
d) Differentiate between information security and computer security [2marks]
e) Describe the following concepts of information security [5marks]

i) Confidentiality
ii) Authentication
iii) Availability
iv) Non-repudiation
v) Integrity

f) Describe the ways of securing information from different threats (8 marks)

g) Distinguish between data and information [2marks]

SECTION B (ANSWER ANY TWO QUESTIONS)

Question 2 (20 marks)

a) Describe the following in relation to computer security threats [10marks]
i) Employee sabotage
ii) Malicious hackers
iii) Bluesnarfing
iv) Social engineering
v) Human error

b) Describe security measures that can be taken to mitigate the above security threats [10marks]

Question 3 (20 marks)

a) Define what is meant with" disaster recovery plan" [2marks]
b) Describe **three** types of malicious code [6marks]
c) Identify and describe the reasons of performing a risk analysis [8marks]
d) Describe the term denial of service and its causes [4marks]

Question 4 (20 marks)

a) Give **two** different ways that a virus can be spread [2marks]
b) Differentiate between a spyware and a virus [4marks]
c) Differentiate between intrusion detection systems and firewall [4marks]
d) Differentiate between encryption and authenticity [4marks]
e) Discuss different attacks that can cause threats to information [6marks]

Question 5 (20 marks)

a) Discuss various ways of disaster recovery plan

[4marks]

b) Describe the procedure of disaster preparedness

[8marks]

c) Describe the policies of disaster preparedness

[8marks]