



THE MOMBASA POLYTECHNIC UNIVERSITY COLLEGE

(A Constituent College of Jkuat)

Faculty of Engineering and Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

HIGHER DIPLOMA IN COMPUTER STUDIES – HDIP 2K 9A

EIT 3209 : COMPUTER SECURITY

END OF SEMESTER EXAMINATIONS

SERIES: AUGUST/SEPTEMBER 2011

TIME: 2 HOURS

Instructions to Candidates:

You should have the following for this examination

- *Answer booklet*

Answer question **ONE (COMPULSORY)** in section **A** and any other **TWO** questions from section **B**

This paper consists of **THREE** printed pages

SECTION A (30 marks)

Question 1 (Compulsory)

- a) Explain the term Computer security (2 marks)
- b) List **FIVE** computer hardware security measures (5 marks)
- c) Explain the importance of computer care (4 marks)
- d) List **FIVE** precautions that can be taken when handling disks (5 marks)
- e) Explain the difficulty experienced in detecting
 - (i) Theft of software
 - (ii) Theft of data (4 marks)
- f) Outline **FOUR** Health and Environmental risk minimization measures in a computer environment (4 marks)
- g) Explain the application of the following management techniques in improving the security of a system
 - (i) Threat monitoring
 - (ii) Audit log (4 marks)
 - (iii) Describe the operations of standard devices used to protect a computer system from power supply interactions (2 marks)

SECTION B (40 marks)

Question 2 (20 marks)

- a) Explain **FIVE** ways in which the computer virus spreads (10 marks)
- b) List **FOUR** ways of protecting software from virus (4 marks)
- c) Explain **THREE** physical measures taken to ensure computer hardware security (6 marks)

Question 3 (20 marks)

- a) State **FIVE** underlying security threats posed to contemporary Electronic Data Processing department (5 marks)
- b) State **FIVE** strategic measures you would recommend to deter the security threats in (a) above (5 marks)
- c) Identify **FIVE** computer software security measures (5 marks)
- d) Identify steps of troubleshooting a computer system (5 marks)

Question 4 (20 marks)

- a) Distinguish between the business continuity plan (BCP) and the disaster recovery plan (DRP) (4 marks)
- b) Distinguish between the **THREE** main security goals (4 marks)
- c) Define the following terms as applied to computer security (8 marks)
 - (i) Cracker
 - (ii) Sneakernet
 - (iii) Firewall
 - (iv) Authentication
- d) Explain any **TWO** measures that can be used to protect users from cyber crime (4 marks)

Question 5 (20 marks)

- a) Define industrial espionage (2 marks)
- b) Explain measures to prevent occurrence of Industrial espionage (5 marks)
- c) Explain plausible cyber terrorism scenarios (4 marks)
- d) Explain dangers posed by cyber terrorism (5 marks)
- e) Explain any **TWO** measures to prevent Denial of Service attacks (4 marks)