



JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING
UNIVERSITY EXAMINATION FOR THE DIPLOMA IN LINUX ENGINEERING
2ND YEAR 2ND SEMESTER 2018/2019 ACADEMIC YEAR
KISUMU CAMPUS

COURSE CODE: ICT 2214

**COURSE TITLE: FUNDAMENTALS OF INFORMATION TECHNOLOGY SECURITY
ENGINEERING**

DATE: 13/08/19

EXAM SESSION: 9.00 – 11.00 AM

TIME: 2.00 HOURS

INSTRUCTIONS

- 1. Answer Question 1 (Compulsory) and ANY other TWO questions**
- 2. Candidates are advised not to write on the question paper**
- 3. Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION 1 [30 MARKS]

- a) What are the goals of security? (3 marks)
- b) Describe the principles of security (6 marks)
- c) Explain the difference between active and passive attacks (4 marks)
- d) Explain the difference between policy, standards and practices (6 marks)
- e) Describe the examples of the commonly used security models (5 marks)
- f) Explain the difference between logging and auditing? (4 marks)
- g) Describe the difference between law and ethics (2 marks)

QUESTION 2 [20 MARKS]

- a) Discuss any five information security principles of success (10 marks)
- b) Discuss why policies should be considered before security technology is acquired and deployed (6 marks)
- c) Provide examples of policies that available in an organization (4 marks)

Question 3 [20 Marks]

- a) Describe what the following terminologies mean (8 marks)
 - i) Cryptography
 - ii) Cryptanalysis
 - iii) Cryptology
 - iv) Cipher text
- b) Give two examples of commonly used encryption schemes (2 marks)
- c) Discuss the several characteristics of a good cipher (10 marks)

QUESTION 4 [20 MARKS]

- a) Give the meanings of the following acronyms as used in Access Control policies (8 marks)
 - i) DAC
 - ii) MAC
 - iii) RBAC
 - iv) ABAC
- b) Explain what is meant by computer security (2 marks)
- c) Discuss the protection mechanisms in a trusted computing base (10 marks)

QUESTION 5 [20 MARKS].

- a) Discuss the types of law that an IT security practitioner should be conversant with (10 marks)
- b) Discuss the qualities of a good policy (8 marks)
- c) Explain the difference between system logging and application logging (2 marks)