KENYATTA UNIVERSITY

UNIVERSITY EXAMINATIONS 2011/2012

SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

SCT 415: INFORMATION SYSTEM SECURITY

DATE: Monday 16th April, 2012 **TIME:** 11.00 a.m. – 1.00 p.m.

Instructions: Answer Question **ONE** and any other **Two Questions**

Question One (30 marks)

(a) Define the term information security.

(2 marks)

(b) Based on the National Computing Centre specifications state and explain the four principles of security.

(4 marks)

(c) State and explain the four categories into which all the techniques for managing the risk fall into.

(4 marks)

(d) Administrative and physical aspects are related in four areas, explain these four areas.

(8 marks)

(e) Briefly discuss the three questions that must be answered when developing an effective security policy.

(6 marks)

(f) Explain three ways in which the security managers deal with catastrophes due to natural disasters.

(6 marks)

Question Two (20 marks)

(a) In most cases people consider technical controls to be more important than the administrative and physical controls. Briefly explain why this perception is not true.

(5 marks)

(b) In developing an information system security plan it is important to include the security policy of the organization. State and explain issues that the policy should address.

(6 marks)

(c) With aid of a suitable diagram explain how the security requirements in relation to other contents of the security plan can be used to develop the required information system security plan security.

(9 marks)

Question Three (20 marks)

(a) Define the term risk analysis as applied in information systems security aspect.

(2 marks)

(b) State and explain any three reasons that support the use of risk analysis as a tool in creating a security plan.

(6 marks)

(c) You have been appointed as an information systems security officer for your organization. The task given to you is to carry out the risk analysis in the existing computing system. Briefly describe how you will perform the risk analysis exercise.

(12 marks)

Question Four (20 marks)

(a) Explain how the following measures are specially designed to minimize the risk of unauthorized data access and fraud.

(i) Personnel selection
(ii) Segregation of duties
(iii) Effective systems maintenance controls
(iv) Follow-up on access violations

(8 marks)

(b) With aid of suitable example illustrate how disaster contingency plans can be used to enable the organization recover from a disaster.

(4 marks)

(c) Explain the physical security techniques that can be used to provide protection on following aspects of the information systems installation.

(i) External building safeguards and barriers.
(ii) Media protection
(iii) Output security
(iv) IT equipment protection

(8 marks)

Question Five (20 marks)

(a) A patent protects inventions and encourages inventors to innovate by granting the patent holder exclusive rights to the invention for 20 years. Explain any five rights a patent owner has.

(10 marks)

(b) A trademark is a word, name, symbol or device used to distinguish one company from another. One to decide on whether infringement has occurred on a trademark or note, what factors should be considered.

(10 marks)