# MACHAKOS UNIVERSITY COLLEGE

**(A Constituent College of Kenyatta University)**
**University Examinations for 2015/2016 Academic Year**

**SCHOOL OF ENGINEERING AND TECHNOLOGY**

**DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY**

**SECOND SEMESTER EXAMINATION FOR DEGREE IN BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**

**SIT 302: INFORMATION SYSTEM SECURITY**

**Date: 1/8/2016** **Time: 2:00 – 4:00 PM**

**INSTRUCTIONS:**

Answer **question ONE and any other TWO questions**

**QUESTION ONE (30 MARKS)**

a) Define the following security related terms:
   i) Integrity (2 marks)
   ii) Availability (2 marks)
   iii) Vulnerability (2 marks)
   iv) Threats (2 marks)

b) i) State three types of firewall (3 marks)
   ii) Describe each of the above firewall types (6 marks)

c) Distinguish between authentication and authorization (2 marks)
d) Explain four basic risk control strategies (8 marks)
e) List any three information security policies (3 marks)

**QUESTION TWO (20 MARKS)**

a) A denial of service attack can take three forms, list and briefly explain each one of them. (6 marks)
b) Explain the two authorization mechanisms applied in information systems (4 marks)
c) The probability of an undesired event causing damage to an asset can be high in any organization. Describe three steps that can be used to lower this probability (6 marks)

d) Explain four information security components. (4 marks)

**QUESTION THREE (20 MARKS)**

a) Differentiate between physical security control and administrative security control giving examples of each. (3 marks)

b) Discuss the disadvantages of a biometric based authentication system giving examples (5 marks)

c) Discuss the following attacks on information systems, stating clearly at least one solution to these attacks. (12 marks)

i) Brute force attack
ii) Dictionary attack
iii) Repudiation attack
iv) Cryptanalysis attack

**QUESTION FOUR (20 MARKS)**

a) Briefly explain the following information and communication types of security breaches (4 marks)

i) Spamming
ii) Data diddling
iii) Spoofing
iv) Phishing

b) Explain four functions information security performs for an organization. (8 marks)

c) i) Define mitigation (2 marks)

ii) Explain three types of plans associated with mitigation. (6 marks)

**QUESTION FIVE (20 MARKS)**

a) Emma is the leader of a project involving 10 other participants in 10 countries. They communicate exclusively by e-mail across a public network. It is important that the authenticity and integrity of message received by participants and purporting to originate from Emma be assured.

Explain how this security requirement may be violated by intruders on the network. (6 marks)

b) Explain the security systems development life cycle. (6 marks)

c) Explain four ways to categorize controls. (8 marks)