JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE THE MASTERS OF INFORMATION TECHNOLOGY SECURITY AND AUDIT

1ST YEAR 3RD SEMESTER 2016/2017 ACADEMIC YEAR

COURSE CODE: IIT 5211

COURSE TITLE: SECURITY POLICIES, STANDARDS, AND COMPLLIANCE STRATEGIES

EXAM VENUE: KISUMU LEARNING CENTRE STREAM:

DATE: EXAM SESSION:

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other three 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 One

Consider these practices:

1. Assess risk and determine needs
2. Establish a central management focal point
3. Implement appropriate policies and related controls
4. Promote awareness
5. Monitor and evaluate policy and control effectiveness

In the light of your own experiences or knowledge of the IT industry. Specifically identify those which are NOT given much attention, and speculate as the consequences of that

(20 marks)

Question Two

a) From your own life experiences – whether in a work environment, educational context, or other less formal setting –identify and describe situation(s) where you feel you may have (without realising it) employed either double-loop learning and/or Kolb's Learning Cycle individually

(14 marks)

b) Discuss how organisations can enthuse their staff to commit to organisational goals

(6 marks)

Question Three

c) Discuss the policy lifecycle

(8 marks)

a) Distinguish between a policy, a standard, a baseline, a procedure, a guideline, and a plan

(6 marks)

b) Using a practical example, discuss why organizations choose to adopt a security framework

(6 marks)

Question Four

a) Using an industry example, provide a road map for the implementation of an international standard

(5 marks)

b) Evidence the intent of ISO/IEC 27000-series of information security standards

(5 marks)

c) Describe information security-related roles and responsibilities

(5 marks)

d) Suggest three polices related to information security policy, governance, and risk management

(5 marks)

Question Five

a) With an appropriate industry example, define the concept of physical security and how it relates to information security

(6 marks)

b) Using an industry you are familiar with, evaluate the security requirements of facilities, offices, and equipment

(6 marks)

c) Develop three policies related to systems acquisition, development, and maintenance

(6 marks)