JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN SECURITY AND FORENICS

3rdYEAR 2nd SEMESTER 2016/2017 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3323

COURSE TITLE: INFORMATION SYSTEMS CONTROL AND AUDIT

EXAM VENUE: **STREAM: Computer Security and Forensics**

DATE: APRIL 2017 **EXAM SESSION:**

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 ONE [30 MARKS

a) What is an Insider Threat, why is it considered the most dangerous within an information system setup, suggest two ways in which you can deal with it? **(4marks)**

b) Distinguish between incidence and incidence response **(2marks)**

c) State the five step Guideline for Collecting Computer Evidence **(5marks)**

d) Distinguish between a Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) **(3marks)**

e) State and briefly explain at least 4 Examples of Common Security Policies **(4marks)**

f) Briefly explain three major ways in which audit trails can be used to support security objectives **(3marks)**

g) What are the three important things that you are required to know before evaluating a risk associated with information systems? **(3marks)**

h) A logic bomb is designed to lay in wait and deliver their payload when logical conditions are met. Using examples briefly describe at least four of these logical conditions **(4marks)**

i) What are some of the technical controls you can advise to be placed within a *network setting* and a *host setting* respectively? **(2marks)**

QUESTION TWO [20 MARKS]

a) The challenge of keeping information systems secure has never been greater, not only because of the number of attacks but also because of the difficulties faced in defending against these attacks. Briefly explain at least 10 reasons despite crafting and implementing controls, it's becoming increasingly difficult to mitigate attacks on information systems **(10marks)**

b) Distinguish between Link and End-to-End Encryption **(4marks)**

c) Briefly describe six types of vulnerabilities that a threat can exploit within an information system. **(6marks)**

QUESTION THREE [20 MARKS]

a) Briefly explain at least six set of skills that is generally expected of an information systems auditor **(6marks)**

b) Discuss the two main categories of data management controls and how they can be implemented **(4marks)**

c) When you are accessing an information system what are the aspects within it that would help you conclude it's a secure system **(3marks)**

d) Passwords are one of the mechanisms of information systems access control it is advised that they shouldn't be the sole mechanism employed. Give reasons to justify the advice **(7marks)**

QUESTION FOUR [20 MARKS]

a) Briefly explain at least six incidence that would face information systems in relation to security **(6marks)**

b) Explain at the goals/aims attributed incidence response within and information system setup **(8marks)**

c) Briefly explain five fundamental security principles that are usually put into consideration when crafting defenses for information systems **(5 marks)**

d) A corporation is considering a best authentication method for access control, which method has the best authentication strength? **(1mark)**

QUESTION FIVE [20 MARKS]

a) Explain at least five major risks relating to personal computers and explain at least five security measures that could be exercises to overcome those risks **(10marks)**

b) With relevant examples briefly elaborate on two administrative, physical and technical controls (**6marks)**

c) Risk is a situation that involves exposure to some type of danger which Information systems are not immune to, as a Information security professional advice on the various different options available when dealing with risks facing information systems **(4marks)**