BONDO UNIVERSITY COLLEGE

UNIVERSITY EXAMINATION 2012/2013

1ST YEAR 1ST SEMESTER EXAMINATION FOR DIPLOMA IN LINUX ENGINEERING

(KISUMU LEARNING CENTRE)

COURSE CODE: ICT 2214

TITLE: FUNDAMENTALS OF IT SECURITY ENGINEERING

DATE: 10 /12/2012 TIME: 10.00-11.30AM

DURATION: 1.30 HOURS

INSTRUCTIONS

1. **This paper contains TWO sections**
2. **Answer ALL questions in section A (Compulsory) and ANY other 2 Questions in section B**
3. **Write all answers in the booklet provided**

SECTION A
QUESTION ONE

a) With an aid of a diagram, describe the concept of security in depth (6 Marks)
b) Explain any **FOUR** strategies that a typical Defense in depth must contain (8 Marks)
c) Assuming you are a network administrator, List **SIX** things you need to know to protect your network (6 Marks)

SECTION B
QUESTION TWO

a) What do you understand by the following terms:
   i. Access Control
   ii. Authentication
   iii. Non Repudiation
   iv. Privacy
   v. Confidentiality (10 Marks)
b) The following are some of IT security compliance solutions; discuss them in detail showing who should comply with them
   i. SOX
   ii. HIPPA
   iii. GBLA
   iv. PCI
   v. COBIT (10 Marks)

QUESTION THREE

a) Differentiate between Symmetric and Asymmetric key cryptosystem (4 Marks)
b) State and explain any **TWO** problems with secret key cryptography (4 Marks)
c) Using transposition cipher of 5, and supposing Alice wants to send the following message to Bob **"enemy attacks tonight"**.Use the following key to find the cipher text

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption (6 Marks)

d) Discuss the **THREE** core principles of IT Security (6 Marks)

QUESTION FOUR

a) With an aid of a diagram, explain the risk management process (6 Marks)
b) After identifying and quantifying risks, one must decide how to respond to them. Discuss the **FOUR** main response strategies for negative risks. (8 Marks)
c) Draw and explain a simple risk matrix showing likelihood (probability) of occurrence and their impact. (6 Marks)

QUESTION FIVE

a) List any **FOUR** natural disasters that may affect IT Infrastructure (4 Marks)
b) Name and explain any **FIVE** IT Security best practices (10 Marks)
c) Describe any **THREE** types of Security attacks (6 Marks)