JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

3RD YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: **IIT 3313**

COURSE TITLE: **LEGAL ISSUES, ETHICS AND INCIDENT RESPONSE IN IT SECURITY**

EXAM VENUE: **STREAM: BSC COMP SECURITY**

DATE: DECEMBER 2016 **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) Explain ANY FOUR legal aspects of protecting IT assets in an organization. [4 Marks]

(b) Comment on the law enactment efforts that has been made to safeguard digital assets by the Kenyan government. [2 Marks]

(c) Classify the following occurrences as an incident or disaster. If an occurrence is a disaster, determine whether or not business continuity plans would be called into play. Comment also on the steps necessary to restore operations and whether in each case law enforcement would be involved. [8 Marks]

(i) A hacker gets into the network and deletes all the files from a server.

(ii) A disgruntled employee takes a critical server home, sneaking it out after hours.

(iii) A fire breaks out in the server room and sets off sprinklers on that floor. Some computers are damaged, but the fire is contained.

(iv) Employees go on strike, and the company could be without critical workers for weeks.

(d) Using a suitable company of your choice, identify the responsibilities of one of the members of the Computer Security Incident Response Team (CSIRT). Consider any four activity lines. [4 Marks]

(e) Below are statements that are either **true** or **false**. For each case, explain the choice of your answer. [4 Marks]

(i) Employees constitute one of the greatest threats to information security

(ii) Risk management is a management function rather than a technical function.

(f) Using a suitable example, explain ***transference***, ***acceptance*** and ***avoidance*** as applies to risk management strategy of IT assets in an organization. [6 Marks]

(g) Explain your understanding of ***probabilistic risk analysis***. [2 Marks]

QUESTION TWO **[20 MARKS]**

(a) Differentiate between *law* and *ethics.* [2 Marks]

(b) Name and explain ANY FOUR metrics that can be considered in handling incident response in IT security. [8 Marks]

(c) Explain the composition and roles of key members of the Computer Security Incident Response Team (CSIRT). [10 Marks]

QUESTION THREE **[20 MARKS]**

(a) Explain the following as applies to *mitigate control strategy* in IT security. [3 Marks]

(i) Incident Response Plan

(ii) Disaster Recovery Plan

(iii) Business Continuity Plan

(b) Identify the TEN key focal areas that need to be considered when instigating a successful incident response plan. [10 marks]

(c) Using a case study of your choice, implement an incident response plan. [7 Marks]

QUESTION FOUR **[20 MARKS]**

(a) Explain the following as applies to risk management of IT assets. [6 Marks]

(i) Risk appetite

(ii) Competitive advantage

(iii) Risk Matrix

(b) Based on potential misuse or embarrassment, organizational data can be classified as confidential, sensitive but unclassified, or public. Identify and classify information that may be contained in;

(i) the desktop PC of the CEO's Secretary [3 Marks]

(ii) Personal Digital Assistant of the company CEO [3 Marks]

(c) "The goal of information security is to reduce risk, the amount of risk unaccounted for after the application of controls and other risk management strategies, to an acceptable level". Discuss. [8 Marks]

QUESTION FIVE **[20 MARKS]**

(a) Differentiate between **Hazard and Operability Analysis (HAZOP)** and **Process Hazards Analysis (PHA)**. [4 Marks]

(b) Determine the applicability of copyright laws in the following cases below; [8 Marks]

(i) Mary has a bought a copyrighted CD and want to load it into an MP3 player. She purchases a software that converts a CD tracks into MP3 tracks.

(ii) Peter has brought a program that he would like to enhance. He uses a dissembler to get the source code from the executables.

(iii) Jerusha made a copy of some gospel music and gave it to her parents as a gift during one of the family reunion event.

(iv) Makiya selects a bunch of folksongs, none of which he wrote, and creates a CD to sell.

(c) "Probabilistic analyses include techniques that can be applied formally to address both *uncertainty* and *variability*, typically arising from limitations of data, models or adequately formulating the scenarios used in assessing risks". Discuss. [8 Marks]

- END –