JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY & FORENSIC

3RD YEAR 1ST SEMESTER 2018/2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE : IIT 3313

COURSE TITLE : Legal Issue, Ethics and Incident Response in IT Security

EXAM VENUE : STREAM :

DATE : 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) The U.S government issued a new export control policy in January 1997 that shifted focus from maximum allowable encryption strength and encouraged vendors to implement key recovery i.e. the ability of law enforcement officials to retrieve encryption keys from a central database and decode messages if necessary. Vendors that incorporate an approved key recovery mechanism in their products can export encryption of any length; Vendors that do not make the commitment are limited to exporting products with a maximum key length of just 40 bits.

1. Define data encryption as per the above case. **[3 Marks]**
2. Briefly explain under what circumstances privacy and confidentiality of Individuals and organizations can be infringed. **[6 Marks]**
3. Why does data encryption create a dilemma for most governments? **[4 Marks]**
4. Discuss the fair information principles. **[8 Marks]**
5. Discuss the moral dimension of information age. **[5 Marks]**
6. Compare and contrast security incident and computer threats **[4 Marks]**

QUESTION TWO 20 MARKS

a) As the information system manager at JOOUST, you have been told by the DVC administrations to implement an ERP system within the next two years. After several months of investigation you have selected an ERP system from a reputable vendor. The system would address the complete scope of your dear university supply chain management. As a responsible professional security expert you've decided to develop an incidence response Plan before the deployment of the system.

1. Describe five Common Incident Types you would consider in the plan. **[5 Marks]**
2. Highlight six Steps of Incident Handler Methodology? **[6 Marks]**
3. Describe three attacker methodologies you would foresee. **[3 Marks]**
4. Organization must have sufficient detection & monitoring capabilities to detect incidents in a timely manner, as the expert give three detection technologies you would prescribe for the following incident detections. **[6 Marks]**
    i. Proactive detection

ii. Reactive detection

QUESTION THREE 20 MARKS

a) Using an appropriate example describe the approach you would take to ethical decision making. **[10 Marks]**

b) Describe the candidate ethical principles that can be employed in making an ethical decision. **[10 Marks]**

QUESTION FOUR 20 MARKS

a) Describe the kind of protection offered by copyrights, trade secret and patents giving two benefits and two limitations of each for developers of computers software. **[9 Marks]**

b) Discuss giving examples of the values embedded, technology such as the internet. **[6 Marks]**

c) Briefly explain four types of policy approaches that can be taken to control Behaviors on the internet. **[5 Marks]**

QUESTION FIVE 20 MARKS

a) Differentiate between computer crime and computer abuse. **[4 Marks]**

b) Briefly discuss the following types of computer misuse as defined by the English Criminal Law **[8 Marks]**

   (i) Computer fraud
   (ii) Computer Hacking
   (iii) Forgery
   (iv) Pornography

c) Describe briefly how information technology has affected the quality of life in relation to Equity, Access, boundaries and dependence. **[8 Marks]**