JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BSC IN COMPUTER SECURITY AND FORENSIC

4TH YEAR 1ST SEMESTER 2018/ 2019 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: **IIT 3412**

COURSE TITLE: **INFORMATION SECURITY POLICY AND COMPLIANCE**

EXAM VENUE:

DATE: **STREAM: BSC FORENSICS**

TIME: 2 HOURS **EXAM SESSION:**

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 the difference between the following terminologies related to computer policy (4 marks)
   i. ICT policy
   ii. ICT security policy
   iii. Acceptable use of ICT policy
   iv. Privacy policy

b) You have been appointed the chief information security officer in an international corporation that conducts many of its activities online. Your job comes as a result of numerous ICT security breaches originating from within and outside the organization. So you have been given the mandate to reengineer the entire ICT security system.

   Required:
   i. What aspect of security will you give first priority? Give a reason for your answer. (4 marks)
   ii. Explain why it would be necessary for you to understand the ICT security trends of the organization in the recent past. (2 marks)
   iii. As you develop and implement the security programme, what three main goals will you be seeking to achieve? (3 marks)
   iv. Explain how the the organization's human resource policy can influence the implementation of ICT policy? (3 marks)

c) Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology management and IT governance. Explain the five COBIT 5 principles. (5 marks)

d) A good security policy must run in tandem with the legal framework of the governing authority within whose jurisdiction the policy is being implemented and must also comply with industry standards and guidelines.
   i. Explain why the ICT policy must operate in line with the government laws in order for it to be effectively implemented. (2 marks)
   ii. Explain why an organization's ICT system must seek to operate in compliance with the industry standards and guidelines. (2 marks)
   iii. State and briefly explain any one ICT security standard for financial systems that governs use of online payments. (3 marks)

e) You have developed an ICT policy for a public university in Kenya. This policy must have formally approved before it is implemented. State the organ of the university that should approve it and give a reason for your answer. (2 marks)

QUESTION TWO (20 MARKS)

a) Information security policy should indicate how information needs to be classified with respect to confidentiality. Describe a three way classification taxonomy for data confidentiality in a university setup. (6 marks)

b) The Health insurance portability and accountability act (HIPAA) is a US federal law enacted to safeguard the proper use of patients'' data.

   i. In the context of HIPAA, explain the meaning of the following terminologies: privacy, confidentiality, portability and accountability. (4 marks)

   ii. Explain the term protected health information (PHI) (2 marks)

   iii. Explain three HIPAA guidelines for computer use in health institutions (3 marks)

c) Information owners are critical in an organization and their roles must be clearly stated in the ICT policy.

   i. Explain the meaning of information owner in an organization. (2 marks)

   ii. Explain the role he needs to play when external consultants are contracted to offer services that may cause them to handle sensitive data in the organization (3 marks)

QUESTION THREE (20 MARKS)

a) When developing ICT policy, one must consider the business strategy of the organization for which he is developing the policy.

   i. Explain the meaning of business strategy (2 marks)

   ii. Giving specific examples, explain why ICT policy must be aligned to business strategy. (3 marks)

b) An ICT security policy is a living document

   i. Discuss the above statements (2 marks)

   ii. State any four factors would that would cause an organization to review its ICT security policy. (4 marks)

c) The Gramm Leach Bliley Act (GLBA) is a comprehensive, US federal law affecting financial institutions. The law requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information. It is composed of several parts including privacy rule and safeguard rule.

   i. Explain what the two rules portend. (4 marks)

   ii. State any five technical safeguards recommended by GLBA. (5 marks)

QUESTION FOUR (20 MARKS)

a) The ICT policy should state the generic responsibilities of various ICT administrators in the organization. Explain the roles of each of the following administrators.
   i. Network administrator (3 marks)
   ii. Database administrator (3 marks)
   iii. Security administrator (3 marks)

b) Explain the meaning of SOX in relation to US federal laws and what led to its enactment. (3 marks)

c) SOX act focuses on three broad areas listed below. Discuss each of their areas giving specifics. (4 marks)
   i. Internal controls (3 marks)
   ii. Compliance and reporting (2 marks)
   iii. Governance (3 marks)

QUESTION FIVE (20 MARKS)

a) ISO 17799 is a set of controls based on the best practices in information security. Outline and briefly explain the ten key contexts of ISO 17799. (10 marks)

b) Explain the six goals of PCI DSS security standard (5 marks)

a) ITIL views IT Service Management (ITSM) as a lifecycle five phases but no definitive starting and stopping points. Explain these five phases. (5 marks)