JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

School of Informatics and Innovative Systems

MSC. Information Security and Auditing

KISUMU CAMPUS

Academic Year: 2021/2022
Year Two Semester One

Course Code: IIT 5211

Course Title: IT Security Policies Standards and Compliance

Stream: Information Security and Auditing

TIME: 3 H0URS

Instructions:

This paper contains FIVE questions

Answer any THREE questions

Question 1 [20 marks]

a) Define information security policy. **(2 marks)**
b) Distinguish between standards, procedures and guidelines. **(3 marks)**
c) Differentiate between the principle of least privilege and "Need-to-know". **(4 mark)**
d) Identify *three* common attributes of access controls. **(3 marks)**
e) Identify at least *four* main tasks involved in policy development **(4 marks)**
f) Define an acceptable user agreement and identify any *three* components. **(4 marks)**

Question 2 [20 marks]

a) Lake Basin IT consultancy is an organization in Kisumu county that provides IT consultancy services. You have been asked to lead a team of IT professionals to develop a security policy. Briefly discuss at least *ten* components that should be articulated in this document. **(10 marks)**
b) Incident can be costly to companies. Every organization should have an incident response program (IRP) in place and should train employees to report all suspected incidents. Briefly discuss at least *five* activities in IRP. (10 marks)

Question 3 [20 marks]

a) A well-written information security policy is to protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information. Discuss at least *five* things that make an information security policy successful. **(10 marks)**

b) According to the National Institute of Standards and Technology (NIST), "the 'people factor'—not technology—is key to providing an adequate and appropriate level of security." incidences. As a result, NIST developed a Security Training and Awareness (SETA) model. Briefly discuss this model. **(10 marks)**

Question 4 [20 marks]

a) The objective of an information classification system is to differentiate data types. Classification systems are used in government, military, and private sector and all these systems differ. Identify and discus how information is classified by government and the military. **(10 marks)**

b) Standards such as the ISO 27002 and NIST exist to help organizations better define appropriate ways to protect their information assets. ISO 27002:2013 is

a comprehensive set of information security recommendations on best practices in information security, and is organized into several domains. Briefly discuss any *ten* of these domains. **(10 marks)**

Question 5 [20 marks]

a) The objective of the business continuity plan (BCP) is to ensure the organization has the capability to respond and recover from a disaster. Briefly discuss the *three* components of the BCP.

(5 marks)

c) Briefly discuss the role of GLBA, HIPAA, and PCI DSS in the regulation/protection of the customers financial, health and card holder data information. **(15 marks)**