(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2019/2020 ACADEMIC YEAR

MAIN EXAMINATION
YEAR THREE SEMESTER ONE EXAMINATION

FOR THE DEGREE OF
BACHELOR OF SCIENCE
(INFORMATION TECHNOLOGY)

COURSE CODE : BIT 313

COURSE TITLE : INFORMATION . ASSURANCE AND SECURITY I

DATE: 11/12/2019 TIME: 11.30 A.M.- 1.30 P.M.

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a. Define the following terms with respect to information assurance and security:

i. Noise (1 Mark)

ii. Information (1 Mark)

ทส. symmetric-key cryptography (2 Marks)

b. Explain how defense in depth security measure can be achieved in an organization. (2 Marks)

c. 'Information assurance is both proactive and reactive…' Explain (2 Marks)

d. Explain the major difference between stream ciphers and block ciphers with respect to symmetric cryptographic algorithms. (2 Marks)

e. Explain what the phrase '*Security is not an absolute; it is a process, not a goal*' means. (3 Marks)

f. Explain how the functioning of an Intrusion Detection System and an Intrusion Prevention System as means for information assurance and security. (4 Marks)

g. The most common way to identify someone is through their physical appearance. something that can not be used to identify someone sitting behind a computer screen or at the ATM. Outline the factors used for authentication to ensure that the person accessing information is, indeed, who they present themselves to be. (3 Marks)

h. 'Using any two authentication factors ensures information is safer compared to using a single authentication mechanism…' Elaborate this statement with the aid of real life scenarios. (4 Marks)

i. Describe one method of multi-factor authentication that you have experienced and discuss the pros and cons of using multi-factor authentication. (6 Marks)

QUESTION TWO [20 MARKS]

a. Outline two different approaches that can be adopted by an organization to implement information security. (2 Marks)

b. Explain the measures that an organization can implement to ensure physical security of the actual hardware and networking components that store and transmit information resources is achieved. (10 Marks)

c. For an organization to be successful, it should have multiple layers of security in place in order to protect its operations. Explain the different categories of security that should be achieved in this multiple layers of security. **(8 Marks)**

QUESTION THREE [20 MARKS]

a. Briefly describe different forms of digital social engineering assaults. **(4 Marks)**

b. Information is created after processing collected data. Briefly describe six characteristics it should possess for it to qualify being termed as useful information. **(6 Marks)**

c. Your exemplary performance in terms of Information Technology has been noticed and that has made the DVC to approach you to give a talk to the subordinate staff at Kibabii University about the major principles of information that have to be protected. Clearly explain the different aspects you will put across. **(10 Marks)**

QUESTION FOUR [20 MARKS]

a. Describe different types of malware attacks which can occur on a computer system without the consent of the user and cause havoc to the computer. **(8 Marks)**

b. Discuss the evolution of information security from the 1960s to present. **(12 Marks)**

QUESTION FIVE [20 MARKS]

a. Layering security defenses in an application can reduce the chance of a successful attack. With the aid of a real life scenario, discuss how this can be made a possibility. **(6 Marks)**

b. Your competency in information technology has enabled you win a consultancy service job of implementing an information security system in an organization which recently was a victim of information security attack as it had no information security system in place. Clearly explain the methodology you will adopt to come up with a comprehensive security posture. **(14 Marks)**