(Knowledge for Development)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2022/2023 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR FOUR SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF
BACHELOR OF SCIENCE COMPUTER SCIENCE

COURSE CODE : **CSC 473E**

COURSE TITLE : **DISASTER RECOVERY**

DATE: 17/04/2023   TIME: 2:00 P.M – 4:00 P.M

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE [COMPULSORY]   **[30 MARKS]**

a, What is an incident in relation to disaster recovery?   [2 Marks]

ii. Determine different strategies in which an Incident Response team can use to stop an incident

and attempt to recover control.   [4 Marks]

b. i. Differentiate between differential and incremental backup.   [2 Marks]

ii. Show any two similarities that exist between the two above   [2 Marks]

c. i. An organization plans against risks that may affect it and it's computing resources. Define

what a risk is.   [2 Marks]

ii. Risk controls operate within one or more of the commonly accepted information security

principles. Identify six principles, beginning with the three basic and detail how they help to

secure an organizations computing resources.   [6 Marks]

iii. Briefly illustrate instances where an organization can validly choose acceptance as a risk

control strategy.   [4 Marks]

d. Describe four causes that are likely to result to loss of data in Kibabii University that will

necessitate data recovery   [4 Marks]

ii. Giving examples and real life illustrations, determine ways in which a disaster recovery team

can classify disasters. Use Kibabii University as a case   [4 marks]

QUESTION TWO: **[20 MARKS]**

a. You are the in charge ICT in your organization. It is a new startup company that doesn't have

a disaster recovery plan in place. Elucidate the relevance of rules, policies, guidelines and

procedures in the development of the disaster recovery plan.   [12 Marks]

b. Interpret to your executive committee why contingency planning is a critical function in the

daily operations of the organization.   [4 marks]

ii. Explain in detail three components of contingency planning   [6 Marks]

QUESTION THREE: [20 MARKS]

a. What is a control strategy and give it importance in disaster recovery   [2 Marks]

b. Contrast between a feasibility study and a cost benefit analysis that will be needed by a business before putting in place a control strategy.   [4 Marks]

c. Your organization has a policy of doing backup at the close of business. You as the network and system administrator are in a board meeting with management which seeks to choose the best backup method. Identify what you will explain to them so that you go with the option of incremental over full backup   [6 Marks]

d. i. Cloud computing is a technology that is currently used as a solution to computing disasters. Give a description of what it entails   [2 Marks]

ii. Identify three major areas of concern in cloud computing and give ways of solving the concerns.   [6 Marks]

QUESTION FOUR   [20 MARKS]

a. As a senior manager in your data backup consultancy organization where students of a local university have visited, give your opinion on types of virtual workplace, what they entails and

their significance in prevention of disasters as a response to a question asked by one of the students. Ensure you detail how the virtual workplace works.   [12 marks]

b. Identify different aspects of a Business Impact Analysis that makes it a crucial reference document for an organization in the event of a disaster.   [4 Marks]

c. Interpret the following techniques as used in secure deletion of data.

   i) Degausing   [2 marks]

   ii) Multiple overwrites   [2 marks]

QUESTION FIVE   [20 MARKS]

a. Identify with detail two types of evidence you will be looking for in a crushed hard disk of a company associated with fraudulent activities   [4 marks]

ii) A client visits your data recovery firm and requests you to inform him on the rules of collecting digital evidence. Interpret to him the different rules that you apply in your duties.

[8 marks]

b. In computing evidence exists in digital format. What are some of the volatile evidence you are likely to collect while collecting digital evidence   [6 Marks]

ii. Detail the steps taken in collection of digital evidence   [2 Marks]