MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2024/2025

THIRD YEAR FIRST SEMESTER FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS

CCF 3301: INCIDENT RESPONSE IN IT SECURITY

DATE: JANUARY 2025 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **ONE** (Compulsory) and any other **TWO** questions*

QUESTION ONE (30 MARKS)

a) State THREE (3) functions of incident handling (3 Marks)

b) Briefly explain the duty of the First Officer Attending (FOA) an incident scene (2 Marks)

c) Define an Incident Management Plan and outline its key components (5 Marks)

d) Explain Locard's Exchange Principle and its significance in investigations. (6 Marks)

e) Outline FIVE (5) possible activities of CSIRTs in Incidence Response process (5 Marks)

f) Distinguish the following terms (6 Marks)

i. Incident and Event

ii. Security Plan and Security Charter

iii. Incident Response and Incident Handling

g) In today's world it is recommended that every organization should have an Incident response policy. Identify the benefits of Incident response policy (3 Marks)

QUESTION TWO (20 MARKS)

a) Discuss the role of Business Continuity Management (BCM) in incident management (6 Marks)
b) Outline FIVE (5) tools and resources for analysis and investigation on cyber incidences (5 Marks)
c) State and briefly explain the TWO (2) general classes of incident analysis to consider during incident response process. (4 Marks)
d) Explain the importance of conducting debriefs post-incident (5 Marks)

QUESTION THREE (20 MARKS)

a) Describe the 5C's of Incident Management in responding to incidents (5 Marks)
b) Discuss the role of hazard analysis techniques like HAZOP and PHA in identifying threats (5 Marks)
c) State FIVE (5) sources of digital evidences in an organization like MUST (5 Marks)
d) During incident tracking process one collects and documents various information. Explain the content of the information captured (5 Marks)

QUESTION FOUR (20 MARKS)

a) Discuss TWO (2) principles of evidence collection in the investigation process (4 Marks)
b) State elements of disaster recovery and business continuity planning (4 Marks)
c) Referencing the Kenyan computer misuse and cybercrimes act, 2018:
   i. Outline any FOUR (4) cybercrime offences that are highlighted in the act (4 Marks)
   ii. Describe the step-by-step investigation procedures highlighted in the act (6 Marks)
d) In dealing with security incidences various Legal and ethical Issues must be considered. Name any TWO (2) of those issues (2 Marks)

QUESTION FIVE (20 MARKS)

a) Every organization aims at achieving security for its data, information, network and information systems. In doing so the organizations follows some laid standards, develops policies and lays down procedures and guidelines to be followed to aid in achieving the security objectives and

minimize the security incidences. Describe what the terms Standard, Policy, Procedure and Guidelines mean in incidence response (4 Marks)

b) Discuss any TWO (2) objectives of Incident Response (4 Marks)

c) Preparation is the first step in creating an incident response plan. Give SIX (6) components of incident preparation (6Mark)

d) Meru University management wants to establish a Computer Incident Response Team and they have called you to advise them on the best option between Outsourcing the Team and establishing an in-house team. Explain the reasons why one would choose any of these options (6 Marks)