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

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

CCF 3401: INFORMATION SECURITY POLICY AND COMPLIANCE

DATE: DECEMBER 2024 **TIME: 2 HOURS**

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

QUESTION ONE (30 MARKS)

a) Define the following terms as used in information security policy and compliance (5 Marks)

i. Privacy-enhancing technologies (PET)

ii. Monitoring

iii. Compliance

iv. Audit

v. Privacy

b) Explain any THREE (3) key data protection principles (6 Marks)

c) Describe FIVE (5) considerations to make when implementing Security Policy (5 Marks)

d) Outline FIVE (5) benefits of information security policies to an organization (5 Marks)

e) Referencing the Kenyan DataProtectionAct__No24of2019, explain the meaning of data commissioner, data controller, data processor and data subject (4 Marks)

f) Discuss the challenges organizations face when developing and implementing security policies (5 Marks

QUESTION TWO (20 MARKS)

a) Explain the role of policies, standards, guidelines, and procedures in an organization (4 Marks)

b) Describe the key elements of an effective security policy (4 Marks)

c) Compare and contrast Enterprise Information Security Policies (EISP), Issue-Specific Security Policies (ISSP), and System-Specific Security Policies (SysSP) (6 Marks)

d) Using example differentiate between personal information and sensitive personal information (6 Marks)

QUESTION THREE (20 MARKS)

a) Identify TWO (2) legal issues and two privacy concern that organizations must address in their security policies (4 Marks)

b) State any SIX (6) main components of an ISO 27001-compliant security management system (6 Marks)

c) Security analysts organize the needs of an organization in order to define a security policy. From the policy, they develop and implement mechanisms to enforce security.

   i. Using a diagram, illustrate the security policy life cycle (7 Marks)

   ii. Explain why feedback is important in policy development and implementation (3 Marks)

QUESTION FOUR (20 MARKS)

a) Describe the following options that are used to evaluate protections for mitigating identified privacy risk (4 Marks)

   i. Business impact analysis

   ii. Vendor risk assessment

   iii. Privacy impact assessment

   iv. Privacy re-engineering

b) Explain the concept of "Construct a secure design before coding" as the BEST way to minimize future security and privacy issues in new software development projects (2 Marks)

c) Your organization is transitioning to cloud-based services. Describe the type of security policy that should be implemented before the transitioning exercise (6 Marks)

d) Discuss the audit and compliance strategies used to enforce information security policies and ensure alignment with Kenya's government ICT standards and guidelines. (8 Marks)

QUESTION FIVE (20 MARKS)

a) Briefly describe how can evaluation tools and techniques such as COBIT and ITIL be used to ensure regulatory compliance within an organization? (6 Marks)

b) Discuss PCI, HIPAA, and SOX global standards (6 Marks)

c) Explain the benefits of ISO/IEC 27001 certification for an organization like Meru University (4 Marks)

d) Discuss the NIST security framework and show how it contributes to an organization's security framework (4 Marks)