



10

(KNOWLEDGE FOR DEVELOPMENT)

**KIBABII UNIVERSITY  
(KIBU)**

**UNIVERSITY EXAMINATIONS  
2017/2018 ACADEMIC YEAR**

**END OF SEMESTER EXAMINATIONS  
FIRST YEAR SECOND SEMESTER**

**FOR MASTER OF SCIENCE IN  
INFORMATION TECHNOLOGY**

**COURSE CODE: MIT 822**

**COURSE TITLE: INFORMATION SECURITY  
MANAGEMENT**

**DATE: 13/08/2018 TIME: 10 AM-12 NOON**

---

**INSTRUCTIONS**

**ANSWER QUESTIONS ONE AND ANY OTHER TWO**



**SECTION A (Compulsory – 20 Marks)**

**QUESTION ONE (20 MARKS)**

- a) Distinguish between law and ethics (2 Marks)
- b) Explain what an Information Security Practitioner should do that can minimize the organization's legal liabilities. (2 Marks)
- c) Explain how an Information Security Professional can deter unethical and illegal behaviour of an employee in an organization. (3 Marks)
- d) (i) Explain the responsibility of an information security professional. (2 Marks)  
(ii) Explain an organization's responsibility regarding information security. (3 Marks)
- e) A Crisis Management Plan is designed to ensure the continuation of vital business processes in the event that an emergency or crisis situation should occur.  
Highlight the scope and objectives of a crisis management plan. (4 Marks)
- f) Explain the following types of social engineering attacks, giving an example for each.  
(i) Scareware (2 Marks)  
(ii) Phishing (2 Marks)

**SECTION B (Attempt any two questions – 40 Marks)**

**QUESTION TWO (20 MARKS)**

- a) Explain the following types of law as regards information security management (4 Marks)
- (i) Civil law
  - (ii) Criminal law
  - (iii) The law of tort
  - (iv) Private law
- b) Highlight five key objectives of a contingency plan in an organization (5 Marks)
- c) Explain what the System Development and Maintenance objectives include in the light of the **ISO/IEC 17799** Information s Security Standard (5 Marks)
- d) A cryptographic hash function must be able to withstand all known types of cryptanalytic attack.

Describe three properties that, at a minimum, a cryptographic function must have. (6 Marks)



### QUESTION THREE (20 MARKS)

- a) Highlight three basic rules that must be followed when shaping an ICT policy. (3 Marks)
- b) Distinguish between a mobile hotspot and tethering (6 Marks)
- c) Highlight five drawbacks of **ISO/IEC 17799** (5 Marks)
- d) Discuss the rationale to justify the development of a comprehensive IT plan and an IT vision. (6 Marks)

### QUESTION FOUR (20 MARKS)

- a) Explain the importance of a professional code of conduct in an organization (10 Marks)
- b) Explain the concept of Digital Rights Management (4 Marks)
- c) A number of forms of Intellectual Property are relevant in the context of network and computer security.

Describe three prominent Intellectual Properties in computing (6 Marks)

### QUESTION FIVE (20 MARKS)

- a) Explain three characteristics that make a data communication system effective (6 Marks)
- b) Explain the concept of software engineering in relation to information security. (4 Marks)
- c) (i) Briefly describe the Digital Millennium Copyright Act (DMCA). (5 Marks)
- (ii) Certain actions are exempted from the provisions of the DMCA and other copyright laws. Highlight five such exemptions (5 Marks)