****

**GARISSA UNIVERSITY**

**UNIVERSITY EXAMINATION 2019/2020 ACADEMIC YEAR THREE**

**SECOND SEMESTER EXAMINATION**

**SCHOOL OF PURE AND APPLIED SCIENCES**

**FOR THE DEGREE OF BACHELOR OF INFORMATION SCIENCE**

**COURSE CODE: COM 323**

**COURSE TITLE: INFORMATION SECURITY**

**EXAMINATION DURATION: 2 HOURS**

**DATE: 18/11/2020 TIME: 3.00-5.00 PM**

**INSTRUCTION TO CANDIDATES**

* **The examination has FIVE (5) questions**
* **Question ONE (1) is COMPULSORY**
* **Choose any other TWO (2) questions from the remaining FOUR (4) questions**
* **Use sketch diagrams to illustrate your answer whenever necessary**
* **Do not carry mobile phones or any other written materials in examination room**
* **Do not write on this paper**

**This paper consists of TWO (2) printed pages *please turn over***

**QUESTION ONE (COMPULSORY)**

1. Explain five objectives of information security **[5 marks]**
2. Digital attacks have increased both in numbers and sophistication. Explain the motivating factors contributing to this move **[5 marks]**
3. Network security aims at protecting information on transist. Identify five types of attacks targeting data in transmission and available controls to protect these attacks from escalating **[10 marks]**
4. Explain how the current computer browsers offer protection against web attacks. Which features should be included in future smart phones **[10 marks]**

**QUESTION TWO**

1. Identify five types of threat that can affect a database system **[5 marks]**
2. For each of the following situation, identify the appropriate computer based controls and explain why such controls is chosen :
   1. a national brokerage firm uses an electronic funds transfer (EFT) system to transmit sensitive financial data between locations **[3 marks]**
   2. A busy organization produce massive amount of information daily and its main problem is data loss and illegal modification **[3 marks]**
   3. a small manufacturing firm uses a simple password system to protect its database but finds it needs a more comprehensive system to grant different privileges like read, view, delete or update to different users. **[3 marks]**
3. An organisation has a database server with three disk devices. The accounting and payroll applications share one of these devices and are experiencing performance problems. You have been asked to investigate the problem. Explain the associated risk and suggest means to overcome this problem **[6 marks]**

**QUESTION THREE**

1. Explain the major steps in multi-step attack **[5 marks]**
2. Explain the functionality and limitations of firewall **[5 marks]**
3. Buy Your Own Device (BYOD) is common practice in modern organization where users devices can access company network. Explain the security challenges they impose to the organization and the security mechanism the organization should implement. **[10 marks]**

**QUESTION FOUR**

1. Research has shown that system users are significant threats to the enterprise information security as they are familiar with the infrastructure and has access to information resources.
   1. Explain the various types of user threats and the control measures an enterprise can implement to safeguard its information assets **[5 marks]**
   2. You are requested to develop a user awareness training program. Explain the main contents of user awareness program you will include **[5 marks]**
2. The Independent Electoral and Boundary Commission (IEBC) is mandated to conduct elections in kenya. The IEBC allows voters identification, voters transmission and analysis to be done electronically. Explain the threats and controls you can implement in the system. **[10 marks]**

**QUESTION FIVE**

1. Risk assessment provides organizations with accurate evaluation of the risks to their assets. Explain the steps to undertake while designing a risk assessment model for an ICT department **[5 marks]**
2. Explain five threats and risks in computer operating systems **[5 marks]**
3. Explain how the following authentication systems are implemented
   1. Public key cryptography **[5 marks]**
   2. Digital signatures **[5 marks]**