EXAMINATION FOR COMPUTER NETWORK SECURITY

DURATION: 2 HOURS

Instructions to Candidates

1. This paper consists of **FOUR** questions. Attempt **question ONE (Compulsory)** and any other **TWO** questions.
2. Do not write on the question paper.

QUESTION ONE (COMPULSORY) (30 MARKS)

a. List three types of data confidentiality. (3 marks)
b. Describe the term operational control and cite an example. (3 marks)
c. Name three types of infosec policies that need to be made in order to produce a full infosec policy. (3 marks)
d. Briefly describe the term cryptography. Hence list two cryptographic hash algorithms. (3 marks)
e. Describe the digital signature verification process. (3 marks)
f. Suppose you discover that an intruder has warez in an FTP area that you are aware of. Describe three actions that you can take to discover the identity of the attacker as a forensics expert. (3 marks)
g. List three pros of a reasonably effective intrusion detection system. (3 marks)
h. Briefly describe three limitations of firewalls. (3 marks)
i. Describe what a VPN protects over a public network. (3 marks)
j. Describe (NOT list) any three ethical issues of the information age. (3 marks)

QUESTION TWO (20 MARKS)

a. Describe the relationship between policies, standards, practices, guidelines and procedures. (5 marks)
b. You have been recently contracted by Bazuzu Logistics Inc management to look into the usage of ICT in their organization. The organization has five departments namely HR, finance, logistics, security and management. The management are concerned about privacy and wastage of resources in the organization. The organization has invested heavily in an expensive color line printer, a black and white printer, an internet server, a color line heavy duty printer, desktop devices in every department, and UPS as well as intelligent switches. Staff have been using the color line printers to print their work including documents of a personal nature. Further an examination of the materials that are being downloaded from the Internet clearly indicates most of it is not work related. Management would like the color line printer for their own exclusive use, and the heavy duty line printer to be used for printing only documents that require color printing (and preferably company related work only). The logistics staff should have exclusive use of the heavy duty black and white printer after 4 pm as this is when they require to print materials for the transport officers to distribute to the drivers on dispatch. The finance department should also have priority printing enabled for them on all printers due to invoicing clients. The management would not like to block the Internet entirely but would like staff to practice fair usage when it comes to personal stuff. Lastly management would like the servers to

log all printing being done and also require special permission for anyone to use the printing and internet services after 7 pm; they would like a report of who has accessed what after 7 pm. This report should be sent to the CEO Ms Muteti every Monday at 8 am.

i. What kind(s) of policies would you require to enforce the above requirements? (2 marks)
ii. How many policies do you require to develop to fulfill the requirements? (3 marks)
iii. Hence write down the relevant policies, and include the standards as well the steps that will fulfill the standards. (10 marks)

QUESTION THREE (20 MARKS)

a. Describe the difference between a session key and pre-distribution key. (5 marks)
b. You have been invited as a security expert by Ngumi Moja Consultants to test their encryption software. They would like to know how easy/hard it is for a hacker to intercept a message from their system to one of their clients and decipher it. Cool. You get to work and the first message you intercept reads as follows:
OFM XRNX ILUVYNOCSKLZ YELXLXANRDD JYAL CVKLUBA.
You examine the cipher and based on your knowledge of breaking ciphers you can guess this is either a Caesar or Captain Midnight cipher or at least variant. You show the consultants that you can break the cipher by actually going ahead to do it. Write down what the cipher is in the format X →Y and send the following reply using the same cipher code: THE CIPHER CODE CAN BE IMPROVED. (15 marks)

QUESTION FOUR (20 MARKS)

a. List four disadvantages of VPNs. (4 marks)
a. You are part of a team that is sub-contractor for VPN solutions. Most of the time you weigh between developing a VPN solution in-house for a client or have the client outsource the solution (which of course only gets you a small 'finder fee' for your team). Your most recent prospect is Summertime Investments a company that receives funds and instructions for investments from their clients in the diaspora. They are of the opinion that they should outsource the VPN service despite the fact that they have a state of the art server and communication equipment. Discuss at least four things they should consider before outsourcing. Finally recommend whether they should outsource or not, justifying your recommendation. (12 marks)
b. Describe four steps you would undertake to protect your system and its data should you suspect you are under attack. (4 marks)