JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS

4th YEAR 2nd SEMESTER 2022/ 2023 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1403
COURSE TITLE: INFORMATION SECURITY POLICY AND COMPLIANCE
EXAM VENUE: **STREAM: SECURITY AND FORENSICS**
DATE: **EXAM SESSION:**

TIME:

INSTRUCTIONS

1. **Answer Question 1 (Compulsory) and ANY other TWO questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

Question 1 [30 marks]

You have been asked to lead a team to develop user policies for a new IT startup organization based in Nairobi.

a) Briefly discuss any five user policies you would develop **(10 marks)**
b) Assuming you are developing a password policy discuss five things you would consider when specifying standards and rules for password **(5 marks)**
c) State at least 6 characteristics that determine the success of a security policy **(5 Marks)**
d) Using a diagram discuss a policy hierarchy. Your discussion should include a policy, a standard, a baseline, a procedure, and a guideline. **(10 marks)**

Question 2 [20 marks]

The goal of data security compliance regulations is to help organizations achieve integrity, security and availability of information systems and data. They provide a set of rules and guidelines that help organizations protect their systems and data from security risks. Title 5 of the GLBA specifically addresses protecting both the privacy and the security of non-public personal information (NPPI). Privacy Rule limits the financial institutions disclosure of NPPI to unaffiliated third parties, whereas security guidelines addresses safeguarding the confidentiality and security of customer NPPI and ensuring proper disposal of NPPI

a) What does GLBA stand for? **(2 marks)**
b) Briefly discuss at least four types of orgnizations does GLBA target? **(8 marks)**
c) What does NPPI stand for? **(2 marks)**
d) Identify four things included in NPPI. **(8 marks)**

Question 3 [20 marks]

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.)

a) Discuss any five of the PCI core principles with regard to data protection. **(5 marks)**
b) Discuss any five of the 12 requirements of PCI DSS. **(5 marks)**
c) Identify three common attributes of access control **(6 marks)**
d) Define the "Principle of Least Privilege" Briefly explain why it serves as a strong foundation for any access control policy **(4 marks)**

Question 4 [20 marks]

a) Policies include many different sections and components – Identify any five of these sections. **(10 Marks)**
b) Standards such as the ISO 27002 exist to help organizations better define appropriate ways to protect their information assets. ISO 27002:2013 can provide a framework for developing security policies. Discuss at least 10 domains of the ISO 27002:2013 standard. **(10 Marks)**

Question 5 [20 marks]

a) The Certified Information System Security Professionals certification has ten domains. The ten domains are derived from different topics about information security. List these domains. **(10 marks)**
b) Proper development of information security policies in organizations requires that the organization Create and implement asset classification policies. Information classification is the organization of information assets according to their sensitivity to disclosure. Most commercial classification systems revolve around four classification levels.

i) Briefly discuss the four levels commonly used in commercial organizations. **(5 Marks)**
ii) Briefly discuss the five levels used in government and military organizations. **(5 marks)**