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 1ST SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1403

COURSE TITLE: INFORMATION SECURITY POLICY AND COMPLIANCE

EXAM VENUE:LAB 14 **STREAM: COMPUTER SECURITY & FORENSICS**

DATE:7/1/25 **EXAM SESSION:14-16.00 HRS**

TIME:2 HRS

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 [COMPULSORY] [30 MARKS]

MobiTech Solutions Limited is an innovative Information Technology startup based in Nairobi-Kenya that specializes in developing mobile and web-based applications for a wide range of clients, including Healthcare Providers, Financial Institutions, and E-Commerce Platforms. The organization recently secured major contracts that involve handling sensitive customer data and ensuring compliance with local and international data protection regulations such as the Kenya Data Protection and the EU's GDPR. The company is growing rapidly and is facing numerous cybersecurity threats, including data breaches, unauthorized access, and insider threats. The Senior Management has recognized the urgent need to implement a comprehensive set of user policies to safeguard the organization's information assets, protect customer privacy, and comply with regulatory requirements. You have been appointed to lead a team responsible for creating these policies and ensuring they align with best practices in information security.

Your task is to develop security policies that will govern employee behavior, define access controls, and ensure that all Information Technology systems are used securely and efficiently. The policies must cover areas such as acceptable use of IT resources, data privacy, password management, incident response, and remote work protocols. You must ensure that the policies are clearly communicated to all employees and that compliance is regularly monitored and enforced. The CEO has also requested that the new policies need to be flexible enough to accommodate the dynamic work environment as it remains robust enough to mitigate security risks. Your approach must be strategic, ensuring that the policies you develop are practical, enforceable, and scalable as the organization continues to grow.

Questions

a) Sketch and develop a detailed security policy for MobiTech Solutions Limited that covers acceptable use of IT resources, password management, and remote work protocols. Your policy should be clear, enforceable, and scalable for a growing organization. **(14 marks)**

b) As the IT Policy and Compliance Lead at MobiTech Solutions Limited, you are tasked identify and justify at least six key elements that must be included in the policy you have developed in (a) above, and briefly explain their importance to the overall security posture of the company. **(6 Marks)**

c) Assuming you are developing a password policy for MobiTech Solutions Limited, discuss five essential considerations when specifying password standards and rules. **(5 marks)**

d) Identify and explain six characteristics that are critical to ensuring the success of MobiTech's security policy. **(5 marks)**

QUESTION 2 [20 MARKS]

a) ISO 17799 is a set of controls based on best practices in information security, designed to help organizations establish, implement, maintain, and continually improve their information security management systems. Outline and briefly explain the key principles or controls included in ISO 17799. **(10 marks)**

b) COBIT 5 is a framework designed to help organizations govern and manage their IT effectively. It was introduced by ISACA to provide practical guidance to ensure that IT aligns with business goals and objectives while balancing benefits, risks, and resource use. In 2018, ISACA launched COBIT 2019, a major update that considers the rapidly changing landscape of technology and business. This version builds on COBIT 5 but offers a more flexible approach, allowing organizations to tailor governance frameworks to their unique needs. COBIT 2019 includes new objectives for governance and management, enabling a deeper understanding of how IT can support overall business strategies. One of the standout features of COBIT 2019 is its focus on customization.

Questions

i. Discuss the benefits that organizations would gain from implementing COBIT 2019 **(5 Marks)**

ii. Using this case study, explain at least five key areas of COBIT 2019 that would contribute to the company's success in IT governance and management.

(5 Marks)

QUESTION 3 [20 MARKS]

a) *"An ICT security policy is a living document"*

i. Discuss the meaning of the statement. **(2 marks)**

ii. Identify four factors that might lead an organization to review its ICT security policy.

(4 marks)

b) You have developed an ICT policy for a public university in Kenya. Before implementation, this policy requires formal approval. Identify the university organ responsible for approving the ICT policy and explain why this organ is the appropriate

authority for such approval. **(5 marks)**

c) The Gramm-Leach-Bliley Act (GLBA) is a comprehensive U.S. federal law that affects financial institutions. It requires these institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information. The act consists of several components, including the Privacy Rule and the Safeguards Rule.

i. Explain the implications of the Privacy Rule and the Safeguards Rule under the GLBA. **(4 marks)**

ii. List five technical safeguards recommended by the GLBA to protect customer information. **(5 marks)**

QUESTION 4 [20 MARKS]

a) The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law enacted to safeguard the proper use of patients' data.

i. Explain the meaning of Privacy, Confidentiality, Portability and Accountability in the context of HIPAA **(4 marks)**

ii. Explain the term Protected Health Information (PHI) under HIPAA. **(1 marks)**

iii. Explain three HIPAA guidelines for computer use in health institutions. **(3 marks)**

b) Explain in brief the main goal of PCI DSS security standard **(2Marks)**

c) The Sarbanes-Oxley Act (SOX) focuses on three broad areas to enhance corporate governance and accountability in financial reporting.

i. Discuss the area of Internal Controls under the SOX Act **(4 marks)**

ii. Explain the significance of Compliance and Reporting as outlined in the SOX Act. **(3 marks)**

iii. Discuss the area of Governance within the SOX framework **(3 marks)**

QUESTION 5 [20 MARKS]

a) You recently graduated with a degree in Computer Security and Forensics, and your hard work has not gone unnoticed. The Chair of the Department at the School of Informatics and Innovative Systems (SIIS), Department of Computer Science and Software Engineering, has recommended you for a position at a well-respected non-

governmental organization (NGO) dedicated to promoting cybersecurity awareness and digital safety in the community. In this role, you'll be at the forefront of various initiatives, from community outreach and educational programs to advocating for policies that enhance cybersecurity awareness at the grassroots level. Your expertise in cybersecurity will be crucial as you develop engaging educational materials, conduct workshops, and create programs to help vulnerable populations stay safe online. You'll collaborate with schools, community centers, and local governments to address the growing threat of cyber risks and promote responsible digital behavior. As you settle into your new position, you'll also evaluate the NGO's current cybersecurity practices, pinpoint areas for improvement, and recommend effective strategies.

i. In your new position, what aspect of security will you first prioritize? Provide a reason for your choice. **(3 marks)**
ii. Why is it essential for you to understand the recent cybersecurity trends of the NGO in the recent past? **(4 marks)**
iii. As you develop and implement your cybersecurity awareness programs, what three main goals will you aim to achieve? Discuss **(3 marks)**
iv. Discuss how the NGO's human resource policy might influence the implementation of ICT Policy. **(4 marks)**

b) In your new role at the NGO, it's essential to ensure that the policies you develop run in tandem with the legal framework of the governing authority within whose jurisdiction the policy is being implemented. The policies must also comply with industry standards and guidelines.

i. Explain why the ICT policy must operate in line with government laws to be effectively implemented. **(2 marks)**
ii. Discuss why an organization's ICT system should operate in compliance with industry standards and guidelines. **(2 marks)**
iii. State and briefly explain one ICT security standard for financial systems that governs the use of online payments. **(2 marks)**

END