00187

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 3, Semester 2 (2022)

IE3072 – Information Security Policy and Management

Duration: 3 Hours

November 2022

Instructions to Candidates:

- This paper has FIVE (05) questions.
- Answer all questions in the booklet given.
- The total mark for the paper is 100.
- This paper contains FOUR (04) pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed.

Question 1 (20 Marks)

a. Assume that you have started working as a security consultant for a software development company which has its own hospital automation solution named Hippocrates. The main clients of the organization are from Europe and United States. Hippocrates is an integrated information system created for managing all aspects of a hospital's operations such as medical, financial, administrative, legal, and compliance.

i. Identify the FOUR instances where Hippocrates uses patient health information. (4 Marks)

ii. Evaluate how data security requirements differ in managing electronic heath records for a client in Europe and a client in United States according to the scenarios you have identified in part i. (8 Marks)

b. The information security management practices should be an overall effort from everyone in the organization.

i. For the given scenario in part a, Identify FOUR security responsibilities with respect to your job role at this company. (4 Marks)

ii. Identify FOUR issue specific information security polices, that you require to fulfill these responsibilities mentioned in part i. (4 Marks)

Question 2 (20 Marks)

a. Explain the characteristics that a security policy needs to have for it to be effective in an organization. (4 Marks)

b. "Policy development and management is a task involving the top management of the organization."

Do you agree with this statement. Justify your answer. (4 Marks)

c. ISO 27001 describes that assets can be broken down into the following categories: Hardware, Software, Information, People, Services and Locations.

i. Assume that a Bank is required to create an asset inventory. Identify a minimum of two assets to that belongs to each of the above categories. (6 Marks)

ii. Identify the owners of each of these assets you have identified in part i. (3 Marks)

iii. Select one of the asset categories and identify two potential threats and two vulnerabilities that could pose risks to those assets. (3 Marks)

Question 3 (20 Marks)

a. Write down the objectives of establishing the Payment Card Industry (PCI) Security Standards Council. (2 Marks)

b. MonstorGadgets is an online shopping mall using Visa in collaboration with Barclays Bank. Due to the popularity and demand, the organization created a mobile application. With both channels up and running, the organization received an average of 20,000 steady flow of customers every month. Organization is a proud maintainer of PCI compliance.

i. Identify the type and level of compliance MonstorGadgets needs to maintain. (2 Marks)

ii. At the end of the third quarter of the year, organization realized that the on-premises servers are insufficient to run MonstorGadgets and upgraded to Enterprise E-Commerce Platform from AWS Marketplace. Evaluate the status of the PCI compliance at MonstorGadgets with the introduction of the new addition. (5 Marks)

c.

i. Identify the stakeholders of PCI compliance. (3 Marks)

ii. For the scenario give n part b, propose an approach to implement 3-D security. (3 Marks)

iii. With the aid of a diagram evaluate how card holders' data (CHD) and sensitive authentication data (SAD) should securely transmit through the payment management cycle of MonstorGadgets. (5 Marks)

Question 4 (20 Marks)

Company ABC grants its employees the privilege of purchasing and using smartphones, tablets, and laptops of their choosing at work for their convenience. Company ABC reserves the right to revoke this privilege if users do not abide by the policies and procedures of the company. This is intended to protect the security and integrity of Company ABC's data and technology infrastructure. Limited exceptions may occur due to variations in devices and platforms. ABC employees must agree to the terms and conditions of the organization to be able to connect their devices to the company network.

a. Identify FIVE possible security risks to the organization according to the scenario given above. (5 Marks)

b. Propose the most suitable information security policy that could cover the above requirements of the Company ABC. (2 Marks)

c. Select two of the risks from part (a) above, evaluate how the policy you have proposed in part b would allow organization to withstand against each of those risks. (4 Marks)

d. Security education training and awareness (SETA) plays a pivotal role in successful policy implementation. Based on your evaluation in part (c), design a poster to be displayed at the company vicinity to emphasize the security best practices to overcome the risks. (9 Marks)

Question 5 (20 Marks)

a. Differentiate between critical infrastructure and critical information infrastructure with suitable examples for each. (6 Marks)

b. Critique the importance of public/ private partnership when protecting critical infrastructure.

(4 Marks)

c.

i. Briefly explain the five framework core functions of National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity developed in 2018. (5 Marks)

ii. Evaluate the need to implement the above-mentioned framework in a tired approach. (5 Marks)

--End-of-Question-Paper--