Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 3, Semester 2 (2019)

IE3072 – Information Security Policy and Management

Duration: 2 Hours

October 2019

Instructions to Candidates:

- This paper has FOUR questions.
- Answer all questions in the booklet given.
- The total marks for the paper is100.
- This paper contains FOUR pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed.
- Attach the question paper to the answer booklet at the end.

Question 1 (25 Marks)

a. "Segregation of duties is essential in order to maintain access control in an organization."

Do you agree with this statement? Justify whether the statement is correct or incorrect with suitable examples. (6 Marks)

b. Differentiate between enterprise information security policy, issue specific information security policy and system specific information security policy with suitable examples for each. (9 Marks)

c. Read the case study given below and answer the questions at the end.

SLIIT Information Technology Accessibility Policy

The SLIIT iTAP is a policy that requires all department and faculties of SLIIT to ensure that their web sites, information systems, and information technologies are accessible to people with disabilities. It is accompanied by standards, implementation guidelines, and procurement recommendations.

i. State the purpose of this information security policy. (3 Marks)

ii. List FOUR stakeholders subjected to this policy. (2 Marks)

iii. Recommend a suitable approach to implement this policy within the organization. (5 Marks)

Question 2 (25 Marks)

a. Define critical infrastructure with suitable examples. (5 Marks)

b. "The Computer Emergency Readiness Team (CERT) is established to conduct reactive cyber security services through timely responses to cyber security incidents and mitigate the resulting damage"

Do you agree with this statement? Justify whether the statement is correct or incorrect with suitable examples. (6 Marks)

c. "The proposed National Cyber Security Operations Centre (NCSOC) will provide timely technical assistance on cyber security issues upon the request of any government institution.

Do you agree with this statement? Justify whether the statement is correct or incorrect with suitable examples. (6 Marks)

d. As a security expert propose a methodology to establish and exercise emergency plans.

(8 Marks)

Question 3 (25 Marks)

a. Briefly describe the following with respect to data classification;

i. Identifiability
ii. Sensitivity
iii. Scarcity

(6 Marks)

b. Using the following ISO 27000 data classification metrics classify the information available at SLIIT. (9 Marks)

Category	Description	Sample documents/ records	Marking	Physical & admin controls	Reproduction	Distribution	Destruction/ disposal
Public							
Internal							
Confidential							

c. Explain what is meant by "accounting of disclosure". Provide three instances of information disclosure permitted under HIPAA. (5 Marks)

d. Janani, is a doctor who works at National Hospital, has access to patient information. Mythra, a cardiologist who works at Lanka Hospital, learns that his friend, Ms. Shiwangi, was admitted to National Hospital. Mythra is concerned and wants to help so he asks Janani to see Ms. Shiwangi's medical record. Together, they discuss their findings.

Evaluate whether this is a HIPAA violation. Justify your answer. (5 Marks)

Question 4 (25 Marks)

a. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

i. Propose an approach to protect cardholder data according to PCI DSS standard. (5 Marks)

ii. Assume that your company is using a third-party service provider to store, process, or transmit cardholder data. As a security expert, recommend options for the top management to perform appropriate compliance validation in PCI DSS.

(6 Marks)

b. Explain the following terms with respect to data protection bill of 2019 ;

i. Profiling
ii. Pseudonymization
iii. Cross-border flows of personal data
iv. Data subject

(8 Marks)

c. Evaluate the impact of both on Sri Lankan businesses with reference to the new Data protection bill. (6 Marks)

---End-of-Question-Paper---