Sri Lanka Institute of Information Technology

B.Sc. Special Honours Degree in IT
(Specialization: Cyber Security)

Final Examination

Year 3, Semester 2 (2017)

IT348 – Information Security Policy and Management

November 2017

Duration: 2 Hours

Instructions to Candidates

1. This paper is preceded by a **10-minute** reading period. The supervisor will indicate when answering may commence.
2. This paper contains **FOUR (04) Questions** printed on **FIVE (05)** pages.
3. Answer **ALL** questions on the **ANSWER BOOKLET** provided.
4. The entire exam is worth **100 marks** and contributes **40%** of the final grade.

Question 1 **[Total: 25 Marks]**

a) Describe how policy development process works according to the organizational structure of a business with an example for each. (9 Marks)

b) Access Control Lists (ACLs) are used as technical specifications for System specific information security policies. Briefly explain **FOUR reasons** for using ACLs in technical specifications. (4 Marks)

c) Read the scenario given blow and answer the questions provided at the end.

GlaxoSmithKline plc (GSK) is a British pharmaceutical company headquartered in Brentford, London. Established in 2000 by a merger of Glaxo Wellcome and SmithKline Beecham, GSK was the world's sixth largest pharmaceutical company as of 2015. The company has a primary listing on the London Stock Exchange and is a constituent of the FTSE 100 Index. To ensure the sensitive information of the company, the management has thought of implementing a Human Resource Security Policy for the organization. As a policy maker you are required to answer the following questions to develop the policy.

i. State the **purpose** of this security policy. (2 Marks)

ii. List FOUR types of personnel subjected to the Human Resource Security Policy. (2 Marks)

iii. Explain how to perform personnel screening to be included in Human resource Security policy. (4 Marks)

iv. Explain how to perform personnel termination be included in Human resource Security policy. (4 Marks)

Question 2 **[Total: 25 Marks]**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It provides a framework for establishment of nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.

a) Explain the **Security Rule** explained under HIPAA. (3 Marks)

b) What is Protected Health Information (PHI) explained under HIPAA? (4 Marks)

c) Assuming that HIPAA is applicable in Sri Lanka. Read the following scenarios and answer the questions provided at the end based on your knowledge related to HIPAA.

i. Assume that you're a nurse at the Malabe clinic. This morning you saw 6 year old, Sajith for a strep test. On the way home from work you stop at Cargill's Foodcity for a groceries. Walking through the Fruit and Vegetable section, you run into Sajith's mother, Malini. "I'm so glad I ran into you! Did you get the strep results yet? It would be great if I knew now so I could pick up the prescription tonight, get him started on the antibiotics and back to school sooner".
Can you disclose information/results to Sajith's mother? Justify your answer.
(6 Marks)

ii. Mr. Premarathne is on the phone. He states his wife was in the Hospital yesterday for lab testing and he wants you to tell him the results of the urinalysis immediately. You explain that his wife has individual privacy rights and such information can be disclosed only to her. You suggest he talk directly to her. He is very angry! "I have a right to know since I pay the bills. I'm going to report you for a HIPAA violation." Should you tell him lab test results? Justify your answer.
(6 Marks)

iii. The Out Patient Department (OPD) is crazy busy this morning due to Dengue Apidemic. As a nurse you're running from one crisis to another. Around 11:00 am you finally get a breather and leave for a cup of coffee. While you're usually diligent about securing your computer when you walk away, this time you were so distracted you forgot. Your computer is logged on to two patient records, one of whom is the wife of the hospital administrator who had a miscarriage. When you return from break, a receptionist is sitting at your desk intently reading the screen.
Who is subject to disciplinary action in this case? Justify your answer.

(6 Marks)

Question 3 **[Total: 25 Marks]**

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.

a) With the aid of a diagram explain the **IT Security Learning Continuum** explained in NIST Special Publication 800-50. (12 Marks)

b) NIST Special Publication 800-50 lists a significant number of topics to be covered in an awareness session or a campaign. As the information security campaign manager design a poster to create awareness about **Laptop security while on travel,** addressing both physical and information security issues. (13 Marks)

Question 4 **[Total: 25 Marks]**

a) Critical infrastructure protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. Explain THREE **types of sectors** considered under critical infrastructure protection.

(6 Marks)

b) Explain the **CIP lifecycle** devised by the Department of Defence. (12 Marks)

c) The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.

ABC Company is a retailer accepting card payments from customers is already a PCI DSS Compliant organization. Due to the growing interest of using IT infrastructure, the company has bought a new set of routers and network equipment.

As a security expert, describe what happens to ABCs PCI DSS Compliant status. What would you suggest the company to follow according to PCI DSS? (7 Marks)

---End-of-Paper---