Sri Lanka Institute of Information Technology

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

Final Examination

Year 3, Semester 2 (2018)

IT348 – Information Security Policy and Management

October 2018

Duration: 2 Hours

Instructions to Candidates

1. This paper is preceded by **10 minutes reading period**. The supervisor will indicate when answering may commence.
2. This paper contains **FOUR (04) Questions** printed on **THREE (03)** pages.
3. Answer **ALL** questions on the **ANSWER BOOKLET** provided.
4. The entire exam is worth 4**0 marks** and contributes **40%** of the final grade.

Question 1 [Total: 10 Marks]

a) Distinguish between **Exceptions to Policies** and **Policy Non-Enforcement** with respect to information security policy development and management with a suitable example.

(4 Marks)

b) SLIIT is implementing an electronic voting system to elect committee members of the yearly appointed faculty student bodies (e.g.: FCSC, FESC and FBSC). Only the current students of the relevant faculties are allowed to vote online at a voting website that the university IT department is implementing.

As an information security professional, develop a guideline to assist the development team covering the security attributes (CIA) that need to be considered for the e-voting system.

(6 Marks)

Question 2 [Total: 10 Marks]

Most of us feel that our health information is private and should be protected. That is why there is a federal law (HIPAA) that sets rules for health care providers and health insurance companies about who can look at and receive our health information.

a) Recommend TWO administrative safeguards and TWO Technical Safeguards to Deergayu Hospital's electronic patients health information to be HIPAA Compliant under risk analysis and management provisions of the HIPAA Security Rule. (4 Marks)

b) Using your knowledge, evaluate the following scenarios for HIPAA violations. You are required to clearly prove your claim whether there is a violation or not. (6 Marks)

i. Children's Medical Center of Dallas fails to use encryption on portable devices.

ii. You had emergency surgery and are still unconscious. Your surgeon may tell your spouse about your condition, either in person or by phone, while you are unconscious.

iii. Memorial Hermann Health System disclosing a patient's PHI in a press release to get the public awareness.

Question 3 **[Total: 10 Marks]**

NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, provides guidance for building an effective information technology (IT) security program and supports requirements specified in the Federal Information Security Management Act (FISMA) of 2002 and the Office of Management and Budget (OMB) Circular A-130, Appendix III.

As the information security campaign manager design a poster to create awareness about the **SLIIT Learning Management System (courseweb.sliit.lk),** addressing information security issues. (10 Marks)

Question 4 **[Total: 10 Marks]**

In 2013, the Federal Energy Regulatory Commission (FERC) approved changes and additions to Critical Infrastructure Protection (CIP) Reliability Standards, also known as CIP v5, which are a set of requirements for securing the assets responsible for operating the bulk power system.

a) As a policy maker, justify the need for public-private partnership in CIP. (4 Marks)

b) Propose guidelines to establish emergency plan to carry out CIP for a government.

(6 Marks)

---End-of-Paper---