Information Security Formulation & Implementation
Final examination
2 Hours

A. This examination consists of questions on material taught through the lecture sessions and associated references.
   - **Part A** (20 Marks - 20%) is composed of ten (10) multiple-choice questions;
   - **Part B** (80 Marks – 80%) comprises six (6) questions that require detailed, complete and correct answers. Be concise with your answers using the fewest words possible to provide detailed, complete and correct answers.

B. You are required to provide detailed, complete and correct answers to the questions

C. You must work individually. The order of questions does not correspond with the order of the course material, associated difficulty or importance.

D. This is a closed book examination and no reference materials are allowed in the examination room. No books, no course notes or printouts of any kind. No calculators, no cellphones/smartphones, computers, or electronic devices of any kind. You must turn off any electronic devices and store them under your desk simply having any device (even if turned off) with you during the exam constitutes a violation and will be reported. If you need to borrow a pencil, sharpener, eraser, etc., you must ask a proctor. You are not allowed to directly talk to any of your neighbours in the examination room.

E. Before, during, and at the end of the examination:
   - You are not allowed to leave the examination room during the examination room period, except for visits to the washrooms.
   - Please do not stand up or talk until all examinations are picked up; this also applies to cases where you finish earlier than the allotted period.
   - Ask the proctor questions that are meaningful in the examination context. Ensure that your questions are not probing for answers to the examination questions.
   - If you are found cheating, involved in discussions, talking to other students or causing any kind of disturbance during the examination, then you will be reported to appropriate University officials for violation of examination policy; you will face appropriate sanctions according to the university examination policy.
   - Answers must be properly marked in the answer book with the corresponding question number. Only answers in the answer book will be marked and graded.
   - Return both the answer/question books back to the proctor before leaving the examination hall.
   - You must stop writing when any of the proctors announces that the allotted examination duration has expired.

Part A – Multiple Choice Questions - 20 Marks (Overall 20%)

1. An information security policy is a primary requirement for establishing control in an information systems organization. Which of the following is not a reason why this is the case?

   A. The policy provides the mandate for implementing the security programme elements.

   B. A policy establishes the steps required to put security in place.

   C. A policy sets the expectations for the employee's behaviour regarding security.

   D. A policy establishes the authority and accountability to protect the organization's assets.

2. The following are good guidelines regarding information security in an organization except:

   A. Developed using industry-accepted practices.

   B. Distributed using all appropriate methods to all concerned.

   C. Reviewed, read and understood by all employees.

   D. Formally agreed to by act and approved by law enforcement.

3. In developing effective policies, a risk assessment is essential. Why?

   A. A risk assessment will determine the risks to be mitigated and how they are related to the organization's strategic objectives.

   B. To achieve its strategic objectives the organization must conduct a risk assessment.

   C. Security policies are controls that mitigate risks identified during the risk assessment phase of policy development.

   D. The law, standards and regulations require that organizations conduct risk assessment as the basis of policy development.

4. The statement 'policies are a countermeasure to protect assets from threats' is supported by all of the following statements except:

   A. They exist to inform stakeholders of acceptable behaviour.

   B. Are automated means of enforcement of desirable employee conduct.

   C. Are intended to enhance employee productivity and deter potentially harmful circumstances.

   D. Explicitly state the consequences of failure to comply.

5. To effectively enforce policies, organizations define and implement comprehensive security education, training and awareness programmes. A key purpose of such programmes includes:
    A. Improving awareness of purpose, scope and accountabilities relating to specific policies.
    B. Developing key needed skills to strengthen the organization's information security programme and enhance the chances of its success.
    C. Building in-depth knowledge in information security at the organization.
    D. Pronouncing required access control routines and processes for specific assets in an organization.
6. Which of the following is NOT a performance measure organizations use concerning information security?
    A. The effectiveness of the implementation of an information security policy.
    B. The evaluation of the compliance of non-security personnel in adhering to the information security policy.
    C. The determination of the effectiveness and/or efficiency of the delivery of information security services.
    D. The assessment of the impact of incidents or other security events on the organization or its mission.
7. One of the following is not among the properties of a well-structured policy:
    A. Has clearly stated purposes and objectives.
    B. Is reviewed at a fixed time defined in the policy, albeit regularly.
    C. Has plainly defined terms to ensure there is no ambiguity.
    D. Developed based on a clear risk assessment methodology.
8. Organizations develop intellectual property policies for, among others, one of the reasons:
    A. IP fuels progress – new ideas and creations. Technological advancement depends on continuous development and application of new inventions;
    B. IP rights are intended to benefit end users and help cultivate the market for inventors, artists, scientists and businesses for their investment in effort, time, money, etc. into their works.
    C. IP laws overly favour the creative class at the expense of the end user's rights to access the proceeds of humanity's creativity.

D. IP protection limits the ability of IP owners to trade, lease or license their IP like any other property.

9. Policy compliance is a means of assuring that those policies, once implemented, are adhered to. Policy compliance includes all of the following except:

   A. Responsibility/accountability for assessing compliance.

   B. Performance measures (metrics/indicators) to gauge the degree to which the policy is complied with.

   C. Related processes and procedures for assessing compliance, including the data to be collected.

   D. Mandatory compliance audits to ensure that policies are adhered to.

10. Some proponents of policy compliance measures distinguish between knowledge-based and behaviour-based metrics. All of the following, except one, are examples of knowledge-based metrics.

   A. The proportion of employees who have attended awareness training.

   B. The percentage of employees who have complied with password policies.

   C. The frequency and total number of awareness courses conducted in a year.

   D. The proportion of employees who have passed the mandatory policy-based quiz.

Part B – Short Answer Questions – 80 Marks (Overall 80%)

1. Security Policies (12 marks)
   A. Define what you understand by the term 'security policy' and why is it important.
   B. What is the relationship between a security policy and the corporate objectives of the organization?
   C. Good policies are characterized by some attributes. Identify and describe at least 3 of such attributes.

2. Security education, training, awareness and information security policy. (10 marks)
   A. Explain what you understand by security education, training, and awareness programmes.
   B. Explain how such a programme can help realize the objectives of an information security policy in an organization.

3. Information security policy metrics (18 Marks)
   A. Explain what you understand by the term 'information security metrics'.
   B. What is the purpose of these metrics towards achieving the objectives for which the policies were created?
   C. Explain what you understand by behaviour-related metrics. Give at least two examples of such metrics.
   D. Explain what you understand by knowledge-related metrics. Give at least two examples of such metrics.
   E. In your opinion, which one of these two is preferable? Why?

4. Concerning information security, explain the following terms. Using relevant examples, indicate where they apply in an organization. (12 marks)
   A. A programme security policy
   B. An issue-specific policy
   C. A system-specific policy

5. **Policy Development Life Cycle:** The diagram below captures the policy development lifecycle. You have been tasked to develop an **incident management policy** for your organization. In point form, indicate at least 2 of the key considerations you would take into account at each stage (Risk Assessment, Policy Construction, Policy Implementation, and Policy Monitoring and Maintenance) of the policy development life cycle. (16 marks)

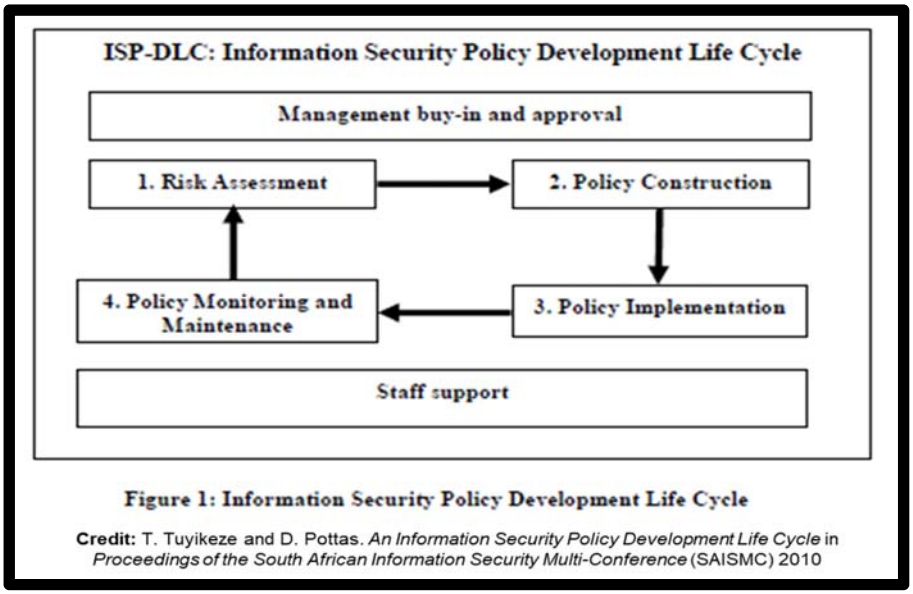

Figure 1: Information Security Policy Development Life Cycle

Credit: T. Tuyikeze and D. Pottas. *An Information Security Policy Development Life Cycle* in *Proceedings of the South African Information Security Multi-Conference* (SAISMC) 2010

6. Organizations take a special interest in adhering to privacy principles. Concerning this answer the following: (12 marks)
   A. Explain the difference between privacy and security as formally defined.
   B. Elucidate why privacy is important
   C. Discuss at least 4 key principles that are essential for privacy.