Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.Sc.(IN-Sc.)/SEM-3/MI-304/2009-10

2009

INFORMATION LAW & POLICY

Time Allotted : 3 Hours Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer any *seven* questions. 7 × 10 = 70

1. a) Define the following terms : 2 + 2 + 2

   Asset, information security and information security management system.

   b) What are the objectives of an information system security program ? 4

2. a) What are the primary and secondary security attributes of enterprise assets ? 4

   b) Explain briefly the interdependence of security attributes of enterprise assets ? 6

3. a) What are the sources of information security requirements for enterprises ? 4

   b) Enumerate and explain the categories of information security threats and vulnerabilities with examples ? 6

4. a) Explain the information security risk management cycle. 4

b) Which of the following is an advantage of qualitative risk analysis over quantitative risk analysis ?

i) It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities of enterprise assets.

ii) It provides specific quantifiable measurements of the magnitude of the impacts of risks.

iii) It makes cost-benefit analysis of recommended controls easier to perform.

iv) What is meant by Information Security Risk Assessment ? 2 + 4

5. Name three qualitative information security risk analysis methods. Explain any *one* of them. 3 + 7

6. a) Define the following terms with appropriate examples : 3 + 3

i) security control.

ii) security policy.

b) Baseline security measures are used to addrss which one of the following ?

i) Specific business needs of enterprise.

ii) Common security control requirements.

iii) Particular information security risk profiles.

iv) A minimum level of loss of enterprise assets. 2

c) Name four well-known information security standards ? 2

7. a) Explain some information security issues of an enterprise. 4

   b) Explain the standard approach to information security risk managment. 4

   c) Define the following terms : 1 + 1

      i) Risk Acceptance.

      ii) Residual Risk.

8. a) Explain the establishment steps of ISO 27001 security standard. 4

   b) How many controls are present in ISO 17799 : 2005 ? 2

   c) Enumerate and explain information security risk treatment options with appropriate examples ? 4