No. of Printed Pages : 3

MSE-024

MASTER OF SCIENCE INFORMATION SECURITY/POST GRADUATE DIPLOMA IN INFORMATION SECURITY

(MSCIS/PGDIS)

Term-End Examination

June, 2024

MSE-024 : POLICY, STANDARDS AND LAWS

Time : 3 Hours *Maximum Marks : 70*

Note : **Section-A :** Question no. 1 is compulsory.
Section-B : Attempt any five question out of seven.

Section–A

1. Write short notes on any four of the following : 5×4=20

   (a) Difference between Cryptography and Cryptanalysis.

   (b) Explain the type of Time stamp with examples.

   (c) Explain various Network related Attacks with examples.

P.T.O.

   (d) Explain how to mitigate the BREACHES of PERSONEL SECURITY.

   (e) Explain the types of attacks on Website. Write the steps to mitigate such attacks as a website administrator.

Section–B

Note : Attempt any five from the rest seven questions.

2. Explain the role of trademarks in protecting brands and consumer interests. What types of symbols or elements can be trademarked, and how do trademarks differ from other forms of intellectual property protection ? 10

3. Explain the concept of copyright protection. What type of creative works are typically covered by copyright, and how does copyright law balance the rights of creaters and the public interest ? 10

4. Discuss the historical significance and contemporary relevance of Section 66A of the Information Technology Amendment Act, 2008 (ITAA 2008), within the context of freedom of speech and expression in the digital age. How has its interpretation and application envolved over time, and what are its implications for online communication and content moderation today ? 10

5. Explain the primary role of ICANN (Internet Corporation for Assigned Names and Numbers), in managing the global domain name system. Additionally, outline both the legal and technical measures an individual or organization can take to protect a domain name from unauthorized use or infringement. 10

6. Discuss the various cybercrimes related to data alteration, destruction, and theft of source code and databases, highlighting their implications for individuals and organizations. Explain how these activities may be considered offenses under the ITAA 2008, and describe the legal consequences and penalties associated with such actions. 10

7. Explain the concept of conventional crimes facilitated by computer technology. Provide examples of such crimes and discuss the challenges in investigating and prosecuting them. How does the integration of technology into criminal activities impact law enforcement efforts and the legal landscape ? 10

8. Cyber terrorism poses a significant threat to national security and critical infrastructure. Explain the key steps and strategies that governments and organisations can take to handle and mitigate cyber terrorism effectively. Discuss the importance of international cooperation in addressing this global issue. 10

***