A-0801

Total Pages : 4 **Roll No. .....**

MIT (CS)-102/CEGCS-02

CYBER SECURITY TECHNIQUES

(MCA/MSCCS/CEGCS)

Examination, June 2025

Time : 2:00 Hrs. Max. Marks : 70

Note* :–** This paper is of Seventy (70) marks divided into Two (02) Sections 'A' and 'B'. Attempt the questions contained in these sections according to the detailed instructions given therein. ***Candidates should limit their answers to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

Section–A

Long Answer Type Questions 2×19=38

***Note* :–** Section 'A' contains Five (05) Long-answer type questions of Nineteen (19) marks each. Learners are required to answer any *two* (02) questions only.

1. What is Information Security and why is it critical for organizations today ? Discuss its key principles (confidentiality, integrity, and availability) and explain how they contribute to the protection of organizational assets.

2. What is the Cyber security Assurance Framework (CSAF) and why is it important for organizations to implement such a framework ? Discuss the components and objectives of the CSAF and how it provides a structured approach to managing cyber security risks in an organization.

3. Explain the concept of "social engineering" in cybercrime. What are the common tactics used in social engineering attacks, such as pretexting, baiting and impersonation? How do attackers exploit human psychology to bypass technical security measures, and what steps can individuals take to protect themselves ?

4. Discuss the relationship between cyber security risk management and governance frameworks such as ISO 27005 and NIST Cyber security Framework. How do these frameworks provide guidance for establishing policies, procedures, and controls to manage cyber risks ?

5. What are the primary tools and techniques used in computer forensics for the collection and analysis of digital evidence ? Discuss the role of imaging software, file recovery tools, and hashing algorithms in preserving the integrity of data during the investigation.

Section–B

Short Answer Type Questions 4×8=32

***Note* :–** Section 'B' contains Eight (08) Short-answer type questions of Eight (08) marks each. Learners are required to answer any *four* (04) questions only.

1. What is Multipurpose Internet Mail Extensions (MIME) and how does it enhance the functionality of email systems ?

2. What is malware and what are the different types of malware commonly used in cybercrime ?

3. Explain the different types of firewalls, such as packet filtering, stateful inspection, proxy firewalls, and next-generation firewalls (NGFW).

4. What are some of the challenges organizations may face when adopting the Cyber security Capability Maturity Model (C2M2) model and how can these challenges be overcome ?

5. What are the main HTTP methods (GET, POST, PUT, DELETE, etc.) and how are they used in web communications ?

6. How can organizations train their employees to recognize and defend against email-based social engineering attacks ?

7. How does the Digital India initiative support cyber security efforts in India ?

8. Write short notes on :

   (a) HSM

   (b) Chat GPT

   (c) Virus

   (d) Disk imaging

****