Roll No. | | | | | | | | | | | | Total No. of Pages : 02

Total No. of Questions : 09

MCA (Sem–2)

INFORMATION SECURITY AND CYBER LAW

Subject Code : PGCA-1932

M.Code : 79619

Date of Examination : 17-06-2023

Time : 3 Hrs. Max. Marks : 70

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION - B & C have FOUR questions each.**
3. **Attempt any FIVE questions from SECTION B & C carrying TEN marks each.**
4. **Select atleast TWO questions from SECTION - B & C.**

SECTION-A

1. Write short notes on :

a) What is the CIA triad in information security?

b) What is information security?

c) What is a vulnerability in information security?

d) What is a threat in information security?

e) What is a risk in information security?

f) What is an exploit in information security?

g) What is a patch in information security?

h) What is an encryption in information security?

i) What is a decryption in information security?

j) What is a password policy in information security?

SECTION-B

2. What is the concept of defense in depth in cyber security and how does it help organizations protect against a variety of threats? What are the different layers of defense in depth, and what security technologies are commonly used to implement each layer?

3. What are the different types of user authentication methods used in information security, and what are the advantages and disadvantages of each method? How can multi factor authentication improve the security of user authentication and what are some best practices for implementing multi-factor authentication in an organization?

4. What is access control in information security and what are the different types of access control mechanisms used to restrict user access to resources in an organization?

5. What are some common methods used by malware creators to distribute and infect systems with malware and what are some best practices for preventing malware infections in an organization? How can malware be detected and removed from infected systems?

SECTION-C

6. What is the difference between a firewall and an Intrusion Detection System (IDS) in information security, and how do they complement each other to protect against security threats? How does a firewall work to control access to a network and what are the different types of firewalls used in modern information security?

7. What are some best practices for implementing an effective intrusion detection system in an organization and how can the results of IDS analysis be used to improve overall security posture?

8. How do encryption and decryption processes work and what are some best practices for implementing cryptography in an organization? What are some common attacks on cryptographic algorithms and how can they be prevented or mitigated?

9. What is the importance of security policies in information security and how do they help organizations establish clear guidelines and procedures for protecting sensitive information? What are some common elements of security policies, such as access control, incident response and data retention and how do they help organizations comply with relevant laws and regulations?

NOTE : Disclosure of Identity by writing Mobile No. or Marking of passing request on any paper of Answer Sheet will lead to UMC against the Student.