

Course Name : MSCCS

Subject Name : Cloud Infrastructure and Services

Subject Code : MSCCS-202

Date : 22-02-2026

Time : 11:30AM TO 01:45PM

Max Marks : 70

Section A

Q.-1. Respond to any three of the following questions in brief. (30)

- (1) Explain Secure Software Development Life Cycle (SSDLC).
- (2) Explain Cross-Site Scripting (XSS) attacks.
- (3) Describe vulnerability assessment techniques.
- (4) Explain cloud security issues and solutions.
- (5) Explain security policies and compliance standards.

Section B

Q.-2. Write short notes on any four of the following topics. (20)

- (1) Explain symmetric and asymmetric cryptography.
- (2) Define application security and what is a security threat?
- (3) Explain CIA triad.
- (4) Define vulnerability assessment.
- (5) What is risk analysis?
- (6) Define disaster recovery.

Section C

Q.-3. Multiple Choice Questions (10)

(1) Application security primarily focuses on:

- | | |
|------------------------|--|
| A) Hardware protection | B) Data protection within applications |
| C) Network cabling | D) Physical security |

(2) Which access control model assigns permissions based on roles?

- | | |
|---------|---------|
| A) DAC | B) MAC |
| C) RBAC | D) ABAC |

(3) Symmetric encryption uses:

- | | |
|--------------------|---------------------|
| A) Two keys | B) One shared key |
| C) Public key only | D) Private key only |

(4) Asymmetric encryption uses:

- | | |
|---------------------|----------------|
| A) One key | B) No key |
| C) Two related keys | D) Session key |

(5) IDS stands for:

- | | |
|------------------------------|----------------------------------|
| A) Internet Detection System | B) Intrusion Detection System |
| C) Internal Defense Software | D) Information Detection Service |

(6) Risk management involves:

- | | |
|-------------------------|-------------------------------------|
| A) Ignoring threats | B) Identifying and mitigating risks |
| C) Data encryption only | D) Hardware upgrades |

(7) Vulnerability assessment aims to:

- | | |
|-----------------------|---------------------------------|
| A) Exploit weaknesses | B) Identify security weaknesses |
| C) Remove users | D) Block traffic |

(8) Ethical hacking is performed to:

- | | |
|-----------------|---------------------|
| A) Cause damage | B) Improve security |
| C) Steal data | D) Hack competitors |

(9) A DoS attack targets:

- | | |
|--------------------|-------------------|
| A) Confidentiality | B) Integrity |
| C) Availability | D) Authentication |

(10) Disaster recovery focuses on:

- | | |
|-----------------------|------------------------------------|
| A) Preventing attacks | B) Restoring systems after failure |
| C) Data encryption | D) User training |

Section D

Q.-4. Decide whether the statements given below are True or False.

(10)

- (1) Application security deals only with hardware protection.
- (2) Confidentiality ensures that data is accessible only to authorized users.
- (3) Security should be considered only during the deployment phase of SSDLC.
- (4) Authentication verifies the identity of a user.
- (5) Symmetric encryption uses two different keys for encryption and decryption.
- (6) IDS stands for Intrusion Detection System.
- (7) Worms require user action to replicate.
- (8) Spyware is designed to secretly collect user information.
- (9) Risk management involves identifying, assessing, and mitigating risks.
- (10) Ethical hacking is performed with the owner's permission.
