

2nd year

B. TECH. (MINOR) CBCS-2023
B. TECH. (MINOR) Semester-I (Sem-III Level) CYBER SEC : WINTER : 2024
SUBJECT: INFORMATION SECURITY

Day : Thursday
Date : 19/12/2024

W-29441-2024

Time : 10:00 AM-01:00 PM
Max. Marks : 60

N.B.

- 1) All questions are **COMPULSORY**.
- 2) Figures to the right indicate **FULL** marks.
- 3) Assume suitable data **WHEREVER** necessary.
- 4) Draw neat diagrams **WHEREVER** necessary.

Q.1 Describe the key implementation and operational issues faced during the development of a secure system. (10)

OR

Q.1 Evaluate the effectiveness of an encryption scheme by discussing its strengths and weaknesses and provide a detailed example of its algorithm. (10)

Q.2 Analyze the potential consequences of security threats on an organization's assets, operations and reputation. (10)

OR

Q.2 Illustrate the process of vulnerability assessment, identifying its key techniques and evaluate the effectiveness of commonly used vulnerability assessment tools. (10)

Q.3 Compare and contrast the characteristics of DAC, MAC, RBAC and TBAC access control models, highlighting their strengths, weaknesses and applications scenarios. (10)

OR

Q.3 Explain multilevel security and trusted computing concepts and develop an implementation strategy for integrating them into a secure cloud service environment. (10)

Q.4 Discuss the role of international standards in shaping information security policies and explain two prominent standards in detail. (10)

OR

Q.4 Summarize the processes involved in the Information Security Department's responsibility for auditing and reviewing security policies for continuous improvement in system security. (10)

Q.5 Analyze the components of database security architecture and evaluate their roles in mitigating vulnerabilities and ensuring the overall security of a database system. (10)

OR

Q.5 Enumerate common software security issues and describes their relevance in the software development process. (10)

Q.6 Explain the key steps involved in developing a business continuity plan that addresses risks from both natural and man-made disasters. (10)

OR

Q.6 Design a case study on the 9/11 tragedy, focusing on the interrelationships between business continuity planning, disaster recovery and information security audits. (10)
