Register Number:……………..

KUMARAGURU
college of technology
character is life

B.E/B.TECH DEGREE EXAMINATIONS: NOV / DEC 2024

(Regulation 2018)

Sixth Semester

INFORMATION TECHNOLOGY

U18ITT6001: Information Security

COURSE OUTCOMES

CO1: Describe threats to information security and security SDLC.

CO2: Identify the security threats and attacks.

CO3: Analyze the mechanism to assess and control risk.

CO4: Describe the types of security policies and standards.

CO5: Identify security issues related to personnel decisions, and qualifications of security personnel.

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 2 = 20 Marks)

(Answer not more than 40 words)

1. Outline the NSTISSC security model's application within modern cybersecurity frameworks. CO1 [K_2]
2. Assess the integration of risk management principles within the Security SDLC. CO1 [K_3]
3. Describe the impacts of common network attacks on organizational security. CO2 [K_2]
4. Evaluate intrusion detection systems' role in mitigating security threats. CO2 [K_3]
5. Analyze the importance of risk assessments in security planning and control. CO3 [K_3]
6. Examine contingency planning's contribution to information security management. CO3 [K_2]
7. Interpret the role of security policies and standards in organizational information security. CO4 [K_2]
8. Analyze the impact of ISO 27001 compliance on security management practices. CO1 [K_2]
9. Identify ethical considerations for information security professionals. CO5 [K_1]
10. Examine the legal ramifications of data breaches under the IT Act, 2000. CO5 [K_2]

Answer any FIVE Questions: -

PART B (5 x 16 = 80 Marks)

(Answer not more than 400 words)

11. a) Analyze the role of Security SDLC in ensuring comprehensive system security from the planning phase to deployment. 8 CO1 [K_4]

b) Discuss the integration of security components into traditional SDLC models. 8 CO1 [K_5]

12.	a)	Describe the impacts of phishing attacks on corporate networks and propose mitigation strategies.	8	CO2	$[K_3]$
	b)	Evaluate the effectiveness of signature-based IDS in detecting phishing and other social engineering attacks.	8	CO2	$[K_5]$
13.	a)	Examine the process of risk identification and assessment for a typical IT Industry.	8	CO3	$[K_4]$
	b)	Propose an improvement plan to current risk management frameworks to enhance cybersecurity resilience	8	CO3	$[K_6]$
14.	a)	Discuss the formulation of information security policies based on ISO 17799/BS 7799 standards.	8	CO4	$[K_3]$
	b)	Analyze challenges organizations face in maintaining compliance with these standards while ensuring effective security.	8	CO4	$[K_5]$
15.	a)	Identify key legal challenges associated with data protection and information security in India.	8	CO5	$[K_4]$
	b)	Discuss the qualifications and roles of security personnel in ensuring compliance with legal standards.	8	CO5	$[K_5]$
16.	a)	Identify a specific security threat that has emerged within the last year. Describe its mechanism and discuss how it challenges existing security protocols	8	CO2	$[K_3]$
	b)	Explain the operation of network-based intrusion detection systems (IDS).	8	CO5	$[K_3]$

****