Reg.No.: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

VIVEKANANDHA COLLEGE OF ENGINEERING FOR WOMEN
[AUTONOMOUS INSTITUTION AFFILIATED TO ANNA UNIVERSITY, CHENNAI]
Elayampalayam – 637 205, Tiruchengode, Namakkal Dt., Tamil Nadu.

Question Paper Code: 5004

B.E. / B.Tech. DEGREE END-SEMESTER EXAMINATIONS – MAY / JUNE 2024
Eighth Semester
Computer Science and Engineering
U19CSE23 – INFORMATION SECURITY
(Regulation 2019)

Time: Three Hours   Maximum: 100 Marks

Answer ALL the questions

Knowledge Levels	K1 – Remembering	K3 – Applying	K5 - Evaluating
(KL)	K2 – Understanding	K4 – Analyzing	K6 - Creating

PART – A

(10 x 2 = 20 Marks)

Q.No.	Questions	Marks	KL	CO
1.	Differentiate vulnerability and exposure.	2	K1	CO1
2.	What is bottom-up approach in Information Security?	2	K2	CO1
3.	Does the Intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?	2	K3	CO2
4.	What measures can individuals take to protect against shoulder surfing?	2	K1	CO2
5.	Define risk management.	2	K1	CO3
6.	Mention a cost benefit analysis.	2	K2	CO3
7.	Define computer forensics.	2	K2	CO4
8.	When is the IR plan used?	2	K3	CO4
9.	Write about honeypot.	2	K1	CO5
10.	Which security protocols are used to protect e-mail?	2	K2	CO5

PART – B

Q.No.			Questions	Marks	KL	CO
11.	a)	i.	Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?	8	K2	CO1
		ii.	Why is a methodology important in the implementation of information security? How does a methodology improve the process?	5		
			(OR)			
	b)	i.	Explain the Systems Development Life Cycle.	8	K2	CO1
		ii.	What multiple layers of security should a successful organization have in place to protect its operations?	5		
12.	a)	i.	What is information extortion? Describe how such an attack can cause losses, using an example.	5	K5	CO2
		ii.	What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?	8		
			(OR)			
	b)	i.	Why is information security a management problem? What can management do that technology cannot?	5	K1	CO2
		ii.	What is privacy in an information security context? What are the major types of attacks used against controlled systems?	8		
13.	a)	i.	What are vulnerabilities? How do you identify them?	6	K3	CO3
		ii.	What is risk appetite? Explain why risk appetite varies from organization to organization. What is residual risk?	7		
			(OR)			
	b)	i.	In support of security efforts, What "The Ten Immutable Laws of Security" are offered by Microsoft?	7	K3	CO3
		ii.	Compare Quantitative Versus Qualitative Risk Control Practices.	6		
14.	a)	i.	What is contingency planning? How is it different from routine management planning? What are the components of contingency planning?	8	K4	CO4
		ii.	What are the five elements of a business impact analysis?	5		
			(OR)			

				Marks	KL	CO

b) i. What are Pipkin's three categories of incident indicators? What is containment, and why is it part of the planning process? — 6 K3 CO4

ii. What are the differences between a policy, a standard, and a practice? What are the three types of security policies? Where would each be used? What type of policy would be needed to guide use of the Web? E-mail? Office equipment for personal use? — 7

15. a) i. What is a vulnerability scanner? How is it used to improve security? What is the difference between active and passive vulnerability scanners? — 6 K5 CO5

ii. What is the fundamental difference between symmetric and asymmetric encryption? What drawbacks to symmetric and asymmetric encryption are resolved by using a hybrid method like Diffie-Hellman? — 7

(OR)

b) i. Define a secure facility. What is the primary objective of the design of such a facility? What are some of the secondary objectives of the design of a secure facility? — 7 K6 CO5

ii. What are the critical considerations when dismissing an employee? Do these change according to whether the departure is friendly or hostile, or according to which position the employee is departing from? — 6

PART – C

(1 x 15 = 15 Marks)

Q.No.	Questions	Marks	KL	CO

16. a) i. Which kind of attack on cryptosystems involves using a collection of pre-identified terms? Which kind of attack involves sequential guessing of all possible key combinations? If you were setting up an encryption-based network, what size key would you choose and why? — 8 K4 CO4

ii. Classify each of the following as a violation of confidentiality, integrity, availability or some combination thereof. Also justify your answer. — 7

    a. Rahul copies Raju's homework.
    b. Ramu crashes Rohit's system
    c. Kajol changes the amount of Jay's check from 100 to 1000
    d. Raani forges saurabs's signature on a deed

(OR)

b) You receive the following E-mail from the Help Desk: K5 CO5
Dear XYZ E-mail User, Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.

*Name (first and last): *E-mail Login: *Password:

*Alternate E-mail:

Please contact the Webmail Team with any questions. Thank you for your immediate attention.

    i.   What should you do? What type of cybercrime is it? Differentiate the passive attacks and active attacks.   8

   ii.   List the security challenges posed by Mobile devices. What are the different types of identity thefts? Define foot printing.   7