Register Number:……..

KUMARAGURU college of technology
character is life

B.TECH DEGREE EXAMINATIONS: APRIL / MAY 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 personal.

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

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1.	What are the components of information system?	CO1	[K_2]
2.	Draw the model of McCumber Cube.	CO1	[K_2]
3.	Write down the four important functions of information security.	CO2	[K_2]
4.	Differentiate law and ethics.	CO2	[K_2]
5.	Give a scenario to explain about man in the middle attack.	CO3	[K_2]
6.	List down the components of risk management.	CO3	[K_2]
7.	Mention the precepts of incident response apply to disaster recovery.	CO4	[K_2]
8.	What do you mean by crisis management?	CO4	[K_2]
9.	Distinguish between false reject rate and false accept rate.	CO5	[K_2]
10.	How does a Mantrap work?	CO5	[K_2]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11.	Summarize the steps performed in both the systems development life cycle and the security systems development life cycle.	16	CO1	[K_2]

12.	a)	Outline the Plan-Do-Check-Act cycle as described by ISO 27000 series.	8	CO4	[K_2]
	b)	In the military, there is a long and distinguished history of generals inspecting the troops under their command before battle, walking down the line checking out the equipment and mental preparedness of each soldier. In a similar way, the security administrator can use vulnerability analysis tools to inspect the units (host computers and network devices) under his or her command. Let discuss the types of scanning and analysis tools used by information security experts in order to secure the network.	8	CO5	[K_4]
13.		"Information security is a major concern for the software industry today as the number of internal threats is nearly 80%" – Discuss on the statement by highlighting the various security attacks and threats.	16	CO2	[K_4]
14.		Classify each of the following occurrences as an incident or disaster. If an occurrence is a disaster, determine whether or not business continuity plans would be called into play. a. A hacker gets into the network and deletes files from a server. b. A fire breaks out in the storeroom and sets off sprinklers on that floor. Some computers are damaged, but the fire is contained. c. A tornado hits a local power company, and the company will be without power for three to five days. d. Employees go on strike, and the company could be without critical workers for weeks. e. A disgruntled employee takes a critical server home, sneaking it out after hours. For each of the scenarios (a–e), describe the steps necessary to restore operations.	16	CO4	[K_3]
15.		Describe the deployment and implementation of Intrusion Detection and Prevention Systems in detail.	16	CO5	[K_2]
16.	a)	Explain the components of risk identification strategy.	8	CO3	[K_2]
	b)	Recognize the existing conceptual frameworks for evaluating risk controls and formulate a cost benefit analysis.	8	CO3	[K_2]

****