Reg. No.:

Name :

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Continuous Assessment Test II – June 2023

Programme	:	**B.Tech CSE**	Semester	:	**Fall Inter 2022-23**
			Code	:	**BCSE353E**
Course	:	**Information Security Analysis and Audit**	Class Nbr	:	**CH2022232501128, CH2022232501125, CH2022232501129, CH2022232501126, CH2022232501120, CH2022232501124, CH2022232501127, CH2022232501122, CH2022232501119, CH2022232501121, CH2022232501118, CH2022232501123**
Faculty	:	**Dr.S.Sandosh, Dr.N.Ganesh, Dr.Padmavathy T V, Dr. Shruti Mishra, Dr.A.Sheik Abdullah, Dr.Joshan Athanesious J, Dr.Sahaya Beni Prathiba, Dr.R.Priyadarshini, Dr.S.Brindha, Dr.S.Abirami, Dr.S. Radhika Selvamani, Dr N.M.Elango**	Slot	:	**TB2**
Time	:	**90 Minutes**	Max. Marks	:	**50**

Answer ALL the questions

Q.No.	Sub. Sec.	Questions	Marks
1.	a	Imagine, you have been hired as a Security Analyst by an insurance firm, and your boss has assigned an initial task to take backup of customer's data. Your role is extended to safeguard the data from the cyber incidents. With insufficient knowledge, your boss has instructed you to take the backup once in a week or month. Now you educate your boss about the importance of taking frequent backups and purpose of every type of backups with suitable examples. (8 marks)	10
	b	Suggest one type of backup which is healthy for your firm with the proper reason. (2 marks)	
2.		Maple organisation provides education as a service. Due to COVID situation, the organisation decided to execute its operations through online mode. Now, the organisation has recruited you as a Chief Security Officer to write specific policies for the following roles, 1. End Users: a) Enterprise Information security program policy (2 policies) b) Issue-specific security policy (2 policies)	10

c) System-specific security policy (1 policy)

2. System Administrator:
   a) Enterprise Information security program policy (2 policies)
   b) Issue-specific security policy (2 policies)
   c) System-specific security policy (1 policy)

3. "Risk Management is an art. Every artist is unique in handling the Risk Management". Assume you are the newly appointed Certified Information Security Manager for a Mobile manufacturing company and you are asked to give a demonstration on how you manage Risks. Frame one Risk and demarcate how you manage it with the utilization of various components. **10**

4. As a security specialist, illustrate the precursors, indicators and response for the following malicious attacks individually, **10**

   a. A virus spread through the email and infect the host (3 marks)
   b. A worm spread through the vulnerable services and infect the host. (3 marks)
   c. A trojan horse is installed and running on host system in the network. (3 marks)

   Also, suggest the containment strategy for the above malwares. (1 mark)

5. Assume you are a Certified Information Systems Security Professional, (CISSP) providing your security service to a top health-care organization. You are maintaining the complete medical records of the patients over several connected devices. Today the management has requested you to train the newly joined System Security Trainees with the Incident Response. As a trainer, you are sharing one former incident of security breach which compromised the organization's network security and deleted some patient records in the database. Illustrate the incident and educate your trainees to protect your network in future from the same incident with the help of response lifecycle. **10**