Name:	
Enrolment No:	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2020

Course:	**Information Security Fundamentals**	**Semester:**	**V**
Program:	**B. Tech CSE+ IT-Infra**	**Time**	**03 hrs.**
Course Code:	**CSSF2001**	**Max. Marks:**	**100**

SECTION A

1. **Each Question will carry 5 Marks**
2. **Instruction: Complete the statement / Select the correct answer(s)**

S. No.	Question	CO
1	According to the CIA Triad, What three security elements are considered in the triad?	CO1
2	When you use the word _____ it means you are protecting your data from getting disclosed.	CO2
3	If a security mechanism offers availability, then it offers a high level of assurance that the data, objects, and resources are _____ by authorized subjects.	CO3
4	LDAP is an example of: – File server – Directory access protocol – Tiered model application development environment – IDS	CO5
5	What is a Log? – An information that records every activity related to any device or application – A process to store data – A procedure to collect event information – A file that stores information of any problem	CO4
6	Which of the following is a Software Asset? – Database – Router – Application – Data Communication	CO1

SECTION B

1. **Each Question will carry 10 marks**
2. **Instruction: Write short/brief notes**

7	Use the key "CODE" to encrypt the sentence "TO BE OR NOT TO BE". Some of the ciphertext is already completed for you: Key C O D E C O D E C O D E C Plaintext T O B E O R N O T T O B E Ciphertext V _ _ _ _ F _ _ _ _ R _ _	CO3, CO4
8	Differentiate between physical and network security. List and explain various physical security threats and controls with examples.	CO2, CO5

9	Write short notes on following technical security controls
	    A. Mantraps
	    B. Turnstiles
	    C. Biometrics
	    D. CCTV surveillance
	    E. Environmental Monitoring controls
		CO4

10	Compare and contrast (a) distributed operating system (OS), (b) batch OS, (c) ral-time OS, (d) time-sharing OS, and (e) network OS.	CO5
11	Define Malware. What are the major categories of malwares. Explain the various solutions for protecting against malwares. **OR** Explain the process of Information Security Audit. List the Auditing & Regulatory Standards used in India. Also, explain the importance of Governance, Risk & Compliance (GRC) framework in it.	CO1

<div align="center">

SECTION C

</div>

1. **Each Question carries 20 Marks.**
2. **Instruction: Write long answer.**

| 12 | Answer any four parts in the following.
   • What is the difference between a private key and a public key?
   • What are symmetric and asymmetric key systems?
   • What kinds of threats exist for a **cryptographic** system?
   • What is polyalphabetic encryption?
   • What is a block cipher?
   • What is cipher block chaining?

<div align="center">**OR**</div>
What requirements must a public key cryptosystem to fulfill to a secured algorithm? What is a public key certificate? What are essential ingredients of the public key directory? Find gcd (1970, 1066) using Euclid's algorithm? | CO2, CO3 |