Seat No.: ________ Enrolment No.__________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (December – 2024)
M.TECH. AI & DATA SCIENCE Semester – I
(SPECIALIZATION IN CYBER SECURITY)

Subject Code: CTMTAIDS SI P3 **Date: 06/12/2024**
Subject Name: INCIDENT RESPONSE AND AUDIT COMPLIANCES
Time: 2:30-5:30PM **Total Marks: 100**

Instructions:

1. Write down each question on a separate page.
2. Attempt all questions.
3. Make suitable assumptions wherever necessary.
4. Figures to the right indicate full marks.

			Marks
Q.1		Attempt any three.	
	(a)	Note down the ways to maximize the CIA triad within the following: I. LAN domain compliance II. Workstation domain compliance	08
	(b)	Write case study related to Cyber IRM.	08
	(c)	What is a Live Response and why it is Preferred for Malware Detection and Containment?	08
	(d)	What is ISO/IEC 27001, and why is it important?	08
Q.2		Attempt any three.	
	(a)	Explain Goals of Incident Response.	08
	(b)	Explain Containment and Eradication.	08
	(c)	How do confidentiality, integrity, and availability (CIA triad) relate to information security?	08
	(d)	Discuss System/Application Domain from IT Domains.	08
Q.3		Attempt any three.	
	(a)	What is PCIDSS and GDPR and Explain it with organization security scenario.	08
	(b)	Explain 1.Precurser and Indicators with Signs of an Incident	08
	(c)	Explain compliance law requirements and business drivers in workstation domain?	08
	(d)	Explain Incident Reporting and Incident Analysis.	08
Q.4		Attempt any two.	
	(a)	How to implement network-based and host-based solutions for IOC creation and searching?	07

	(b)	**Explain Disaster Recovery & planning of DR**	**07**
	(c)	**How vulnerability, threat and attack effects the IT security audit?**	**07**
Q.5		**Attempt any two.**	
	(a)	**Explain Incident Prioritization with example.**	**07**
	(b)	**Elaborate and list the classification of critical control requirements for an IT infrastructure audit.**	**07**
	(c)	**Explain Types of Computer Security Incidents**	**07**

--- End of Paper---