

GUJARAT TECHNOLOGICAL UNIVERSITY**BE - SEMESTER-IV EXAMINATION – SUMMER 2025****Subject Code:3144802****Date:17-05-2025****Subject Name:Cyber Security Law and Compliance****Time:10:30 AM TO 01:00 PM****Total Marks:70****Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.
4. Simple and non-programmable scientific calculators are allowed.

		Marks
Q.1	(a) Explain the issues and challenges of Cyber Security in India.	03
	(b) Explain cybercrime and relevant legal sections.	04
	(c) Discuss the role of the Government Examiner of Digital Evidence in the investigation of cybercrimes. Explain the various sections of the law that govern cybercrimes and the requirement of certification for presenting digital evidence. Explain the report from cyber forensics understood and utilized in legal proceedings.	07
Q.2	(a) Explain the importance of Section 65B of the Indian Evidence Act.	03
	(b) Highlight specific Indian Penal Code (IPC) sections that are used in conjunction with the Information Technology Act to penalize cyber offences.	04
	(c) Discuss the global legal frameworks addressing cybercrimes under international law. Highlight the challenges faced in enforcing cyber laws across different jurisdictions.	07
	OR	
	(c) Provide a brief overview of the Information Technology Act, 2000, highlighting its key objectives and provisions.	07
Q.3	(a) Explain the primary survey in crime scene management.	03
	(b) Explain the role of digital forensics in solving cybercrime cases.	04
	(c) Explain the basic types of evidence in forensic analysis. 1.Visible 2.Plastic 3.Latent 4.Micro & Macro 5.Pattern 6.Trace and Ultra-Trace 7.Fragile and digital evidence	07
	OR	
Q.3	(a) Describe the concept of pattern evidence in a crime scene and its significance in forensic investigations.	03
	(b) Highlight the steps involved in ensuring that evidence is properly identified, collected, and preserved from the crime scene.	04
	(c) Describe the importance of scene photography in forensic investigations and outline the key methods used to ensure comprehensive and accurate documentation of a crime scene.	07
Q.4	(a) Define electronic governance (e-governance). Explain the benefits it provides to citizens and governments.	03
	(b) Define electronic evidence. Lists its key characteristics and explains how is it classified in the context of cybersecurity and law.	04
	(c) Explain the factors involved in determining the best data acquisition method in digital forensics. Discuss commonly used acquisition tools and the importance of validating data acquisitions to ensure the integrity and admissibility of digital evidence.	07
	OR	
Q.4	(a) Explain how the legal recognition of electronic records and electronic	03

	evidence is used in legal proceedings.	
	(b) Explain the significance of digital signatures in ensuring security and authenticity in the cyber world.	04
	(c) Discuss the process of data acquisition in digital forensics, focusing on understanding different storage formats and the handling of digital evidence. Explain the importance of choosing the correct storage format and how it affects the integrity and usability of digital evidence.	07
Q.5	(a) Differentiate: Cyberbullying and Cyberstalking	03
	(b) Briefly explain the role of psychological profiling in identifying cyber offenders. How does it help in preventing cybercrimes.	04
	(c) Discuss the importance of personality profiling in cybersecurity. Explain the application of the Five-Factor Model (FFM) and Dark Triad traits in understanding and managing cybersecurity risks.	07
	OR	
Q.5	(a) Explain the methods used to detect malingering and deception in cybersecurity. How do these techniques help in securing systems.	03
	(b) Define brain mapping in the context of cybersecurity. Explain how brain mapping and signature analysis are used to enhance security systems and detect potential threats.	04
	(c) Explain the importance of psychological assessment in cybersecurity. Discuss how understanding human behavior helps in preventing cybercrimes and the role of psychological profiling in detecting potential cyber threats.	07
