GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Industry Led Minor/Hons.

Level: UG

Branch: Cyber Security

Course / Subject Code: BE04IAQ011

Course / Subject Name: Introduction to Information Security and Cryptography

w. e. f. Academic Year:	2025-26
Semester:	4th
Category of the Course:	Core Courses

Prerequisite:	Basic knowledge of computer Networks
Rationale:	This subject provides a comprehensive foundation in cybersecurity, combining modern technologies, core security principles, IT management, practical skills, and regulatory knowledge. Emphasizing both theory and hands-on practice, it prepares students for real-world security challenges and effective communication in professional settings.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	Understand ITIL Service Lifecycle, processes, and roles.	U
02	Use standardized vocabulary for Service Management.	A
03	Differentiate information security objectives and use jargon.	N
04	Comprehend cryptography types and digital signatures.	U
05	Recognize recent Cyber-attacks and impacts.	R
06	Identify and fix web application vulnerabilities.	A
07	Understand web services and SOA principles.	U
08	Learn about Security Standards and Regulations.	R

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours/week)			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
3	0	2	4	100	0	0	0	100

*Total Lecture Hrs. (L) =45	Total Practical Hrs. (PR) =30.	Total Hours =75 Hrs

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Industry Led Minor/Hons.

Level: UG

Branch: Cyber Security

Course / Subject Code: BE04IAQ011

Course / Subject Name: Introduction to Information Security and Cryptography

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	**Embracing Next Gen Technologies-** Introduction to Cloud Computing, Introduction to Big Data, Introduction to AI and ML, Introduction to IoT and Mixed, Introduction to Cyber security **Fundamental of Information Security** - Introduction, Why Information security? What is Information security? Cryptography, Network security, Application Security, Conclusion	10	20
2.	**Fundamentals of Information Security** - Introduction, Why Information security? What is Information security? Cryptography, Network security, Application Security**, Cryptography Fundamentals** - Why Cryptography? Cryptography, Shared Key Cryptography - Illustration, Shared Key Cryptography, Public Key Cryptography - Illustration, Public Key Cryptography, Hashing, Digital Signature - Illustration, Digital Signature, Applications of cryptography, **Introduction to Cyber security -** Recent Cyber Attacks, Cyber Security Concepts, Layers of Cyber Security	15	20
3.	Introduction, Bloom's Taxonomy, what is service? Types of Services, Governance and management system, ITIL, Service Management, Risk Management, Service Life Cycle, Service strategy, Value creation through Service, Service Portfolio Management, Business Relationship Management, Demand Management and Service Design, Information Security Management, Supplier Management	10	15
4.	Service transition, Transition planning and support, Change Management, Service Asset and configuration Management, Knowledge Management, Challenges, Service Operation, Incident Management, Request Fulfillment, Access Management, Problem Management, Service Improvement, Technology Architecture	10	15
5.	**Introduction to Service Oriented Architecture** - Introduction to Application Security, Secure Coding OWASP Top 10, Coding Practices, Secure Design, What is Service Oriented Architecture, The data and application layer, The enterprise components layer, The services layer, The business process layer, The presentation layer, Introduction to Service Oriented Architecture, **Security Standards and Regulations** - ISMS, FIPS and NIST Special Publications - FISMA, GDPR, HIPAA, SOX, Java SE 11 Programmer II: Secure Coding in Java SE 11 Applications**, Ethical Hacking for Beginners** - Reconnaissance and Scanning What is Reconnaissance?, Working with NMap, Shodan for scanning, Other Types of Reconnaissance, Exploit and Sniffing, Metasploit Basics, Exploiting a Vulnerability, Armitage, Air cracking, MitM (Man-in-the-Middle) Attack, Social Engineering Toolkit, Working with Wireshark	30	30

	Basics of Business Communication - Basics of Business communication, Mechanism of communication, Effective Articulation.		
	Total	**75**	**100**

Suggested Specification Table with Marks: Given here tentative, which may vary as per Author and Course.

Distribution of Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20%	**30%**	**30%**	**10%**	**10%**	

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

Skill & Practical Activities to be carried out during Semester						
Sr. No.	**Category of Engagement**	**Describe the activities to be carried out by students in brief**	**Expected Frequency & Duration**	**Mode of Delivery (Online / Offline / Hybrid)**	**Tools / Platforms / Equipment / Machinery to be Used**	**Expected major Learning Outcomes**
1	Tutorials / Guided Technical Sessions	Complete the lectures	Twice a week	Online	Infosys Springboard platform/app	Apply secure coding principles; Understand vulnerability mitigation
2	Master Classes / Expert Lectures by Industry Professionals	Attend the live class, ask doubt and complete practical	15 Hours	Online	Zoom / MS Teams	Gain industry insights; Understand compliance requirements
3	Quizzes / Competency-Based Evaluation	Complete quizzes on portal	After each module	online	Infosys springboard platform/app	Better understanding about topic

4	Hands-on Training / Lab Exercises / Tool-Based Learning	Lab on secure coding and penetration testing	Weekly, 2 hrs	Offline	OWASP ZAP, Burp Suite	Perform vulnerability scanning; Apply secure coding practices.