Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Faculty of Computer Applications

FACULTY OF COMPUTER APPLICATIONS

Programme	BCA Honors	**Branch**	Computer Applications
Semester	VI	**Version**	1.0.0.0
Effective from Academic Year	2026-2027	**Effective for the batch Admitted in**	June 2024
Subject Code	U36B4ICS	**Subject Name**	INTRODUCTION TO CYBER SECURITY

Teaching scheme						**Examination scheme (Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	4	-	-	-	4	Theory	50	50	100
Hours	4	-	-	-	4	Practical	-	-	-

Objective:

To introduce students to fundamental concepts of cyber security and digital protection.
To develop skills for identifying, preventing, and responding to cyber threats and attacks.

Pre-requisites:

Students should have a basic understanding of computer systems, networking, and the internet.

Course Outcomes :

Name of CO	**Description**
CO1	Understand basic concepts of information security, threats, and attacks.
CO2	Analyze network security, authentication mechanisms, and basics of penetration testing.
CO3	Evaluate social media risks, cyber-crimes, and user-level security practices.
CO4	Apply security principles in mobile, cloud, IoT, and application environments.
CO5	Understand digital forensics, incident response, and evidence handling.
CO6	Explain cyber laws, cyber space, ethical issues, and user awareness techniques.

Mapping of CO and PO

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	0	2	2	1	1	2	3	1	1	0
CO2	2	2	0	3	3	2	2	3	3	1	1	0
CO3	2	2	0	2	2	2	1	2	3	1	1	1
CO4	1	1	0	2	3	3	2	2	2	1	1	1
CO5	2	2	0	3	2	2	1	2	2	1	1	1
CO6	2	1	0	2	2	1	2	2	3	1	1	1

Content:

Unit		Hrs
1	**Introduction to Information Security and Attacks** Basics of Computer Security and its types, Introduction to Information Security, Need for Security, Threats and Attacks: Malicious code, Backdoor, Password Cracks, Brute force, Mail Bombing, Spam, Secure Software Development.	10
2	**Internet Authentication and Network Attacks** Basic concepts of Internet Standards, Principal of security, Authentication Basics: Password, Authentication Token, Certificate-based Authentication, Basics of authentication in Wireless Networks, Types of Network Attacks: DoS (Denial of Service), DDoS (Distributed Denial of Service).	10
3	**Social Media Privacy Issues and Security** Fundamental of Social media privacy, General account settings, Basic and advanced privacy settings, Basics security of Social media, scope of Cybercrime, Categories and Types of Cyber Crimes: Hacking, Phishing, Identity Theft, Cyber Bullying, Online Scams and Frauds, Case studies	10
4	**Application security** Types of cyber security: mobile application security, Application security in cloud, Network security, endpoint security, infrastructure security, internet of things security.	10
5	**Digital Forensics and Incident Response** Role and fundamentals of digital forensics, Incident response process, Laws and rules of evidence, Forensic tools and techniques, Digital Forensic Lab setup, Physical security, Jump kits.	10
6	**Introduction to CyberSpace** Overview of Cyber Space: Definition and significance, Basics of Cyber Law: Understanding the scope and importance, Digital Infrastructure: Importance in the context of cyber law IT Act 2000, Cyber laws, Ethical issues, Prevention techniques and user awareness.	10

Practical Content:

NA

Text Books:	
1	Cryptography and Network Security' by Behrouz A Forouzan, Debdeep Mukhopadhyay,2nd Edition 2010.
2	Introduction to cyber security by Anand shaide
3	Cyber law simplified –viveksood (TMH)
4	Corporate Computer and Network Security by Raymond R Panko, Pearson Publications
Reference Books:	
1	Cyber Security Essentials – Charles J. Brooks et al.
2	Computer Security: Principles and Practice – William Stallings
3	Cyber Security – Nina God bole & Sunit Belapure
4	Cryptography and Network Security Principle 2nd edition by atulkahte.
5	CEH Certified Ethical Hacker Study Guide by Ric Messier Sybex 1st Edition 2019.
Web References / MOOC / Certification Course	
1	https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US
2	https://www.coursera.org/learn/introduction-to-cybersecurity-fundamentals
3	https://www.edx.org/learn/cybersecurity/harvard-university-cs50-s-introduction-to-cybersecurity
4	https://www.edx.org/masters/micromasters/ritx-cybersecurity
5	https://onlinecourses.nptel.ac.in/noc25_cs116/preview

Question Paper Scheme:	
	End Semester Examination Duration: (2 Hours Theory Examination) **Note for Examiner:** - Q-1 Any Five out of Seven (25 Marks) Q-2 Any Two out of Three (06 Marks) Q-3 Mandatory question (05 Marks) Q-4 Any Two out of Three (08 Marks) Q-5 Any Two out of Three (06 Marks) *The question paper must comprehensively address all Course Outcomes (COs), align Taxonomy levels, and ensure complete syllabus coverage.*