Ganpat University ॥ विद्यया समाजोत्कर्षः ॥ | Faculty of Computer Applications | NAAC A Grade Accredited University

Programme	B. Sc. (CA & IT) Honours	**Branch**	Computer Applications
Semester	VI	**Version**	1.0.0.0
Effective from Academic Year	2026-27	**Effective for the batch Admitted in**	June 2024
Subject code	U16B4CS	**Subject Name**	CYBER SECURITY

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

Objective:

To provide foundational knowledge of cyber security concepts, threats, and defense mechanisms to ensure digital safety.

Pre-requisites:

Basic understanding of computer systems and internet usage.

Learning Outcome:

Name of CO	Description
CO1	Understand the fundamentals of cyber security, including its importance, key concepts, principles of data protection, and professional responsibilities.
CO2	Identify various types of cyber threats and attacks, including malware, social engineering, and network-based attacks using real-world examples.
CO3	Understand types of cybercrimes, their impact, and real-world examples like data leaks and online fraud.
CO4	Apply core cyber defense strategies like Defense-in-Depth, firewalls, IDS/IPS, endpoint protection, and cryptographic techniques.
CO5	Follow secure software development practices, including secure coding, SDLC integration, and tools for testing vulnerabilities.

Mapping of CO and PO:

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

Content:

Unit	Content	Hrs.
1	**Fundamentals of Cyber Security** Definition and importance of cyber security, Scope and Emerging challenges, Evolution of cyber threats, Key concepts in cyber security, Principles of Data protection (confidentiality, integrity, availability), Roles and Responsibilities of cyber security Professionals.	12
2	**Cyber Threats and Attack Types** Types of cyber threats, malware (viruses, worms, trojans, ransomware), Social engineering attacks (phishing, spear phishing, baiting), Network-based attacks (DDoS, man-in-the-middle, SQL injection), Case Studies (real-world cyber attacks, breach	12

	analysis, lessons learned).	
3	**Introduction to Cybercrime** Understanding Cybercrime, Link between Cybercrime and information security, Types of cybercrimes (identity theft, cyberbullying, hacking, financial fraud), Cyber offenses (unauthorized access, data breach, cyber terrorism), Examples (Aadhar data leak, social media fraud, banking scams).	12
4	**Cyber Defense Strategies** Introduction to defense strategies, Concept of Defense-in-Depth (layered protection), Basics of Network security (firewalls, IDS [Intrusion Detection System], IPS [Intrusion Prevention System]), Endpoint protection methods (antivirus software, EDR [Endpoint Detection and Response]), Cryptography basics (encryption, hashing, digital signatures), Importance of cybersecurity awareness and training (emails, passwords, social media safety).	12
5	**Secure Software Development** Meaning and importance of secure Development, SDLC steps (plan, build, test, deploy securely), Safe coding (input validation, output encoding, error handling), Security testing (code review, vulnerability scanning, penetration testing), Tools (static and dynamic analysis), Real examples (secure apps, common mistakes)	12

Practical Content:
-

Reference Books:	
1	**Fundamentals of Cyber Security** – By Bhushan Trivedi, Wiley India
2	**Introduction to Cyber Security** – By Chwan-Hwa (John) Wu and J. David Irwin, CRC Press
3	**Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives** – By Nina Godbole and Sunit Belapure, Wiley India
Web Reference:	
1	https://www.ncsc.gov.uk
2	https://www.cisco.com/site/us/en/products/security/index.html
MOOC/Certificate Course:	
1	https://www.futurelearn.com/courses/introduction-to-cyber-security
2	https://www.coursera.org/learn/ibm-cybersecurity-for-beginners
3	https://www.coursera.org/specializations/intro-cyber-security
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 with Bloom's Taxonomy levels, and ensure complete syllabus coverage.