Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Faculty of Computer Applications

NAAC A Grade Accredited University

Programme	B.Sc. IT Honours (Data Science)	**Branch**	Computer Applications
Semester	V	**Version**	1.0.0.0
Effective from Academic Year	2026-27	**Effective for the batch Admitted in**	June 2024
Subject code	U75B5FIS	**Subject Name**	FUNDAMENTAL OF INFORMATION 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 understand and apply concepts and technologies for securing information systems against cyber threats

Pre-requisites:

Basic knowledge of computer systems, networks, and operating systems

Learning Outcome:

Name of CO	Description
CO1	To understand fundamentals of information security and CIA triad.
CO2	To identify threats and apply secure development practices.
CO3	To utilize cryptographic methods and analyze cryptosystem attacks.
CO4	To explore internet security standards and authentication techniques.
CO5	To apply security technologies like firewalls, VPNs, and IDS/IPS.

Mapping of CO and PO:

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

Content:

Unit	Content	Hrs.
1	**Foundations of Information Security:** Introduction to Information Security, Basics of Computer Networks relevant to Security, Fundamentals and Objectives of Computer Security, Types of Security, CIA Triad (Confidentiality, Integrity, Availability), Information Systems in Security Context, Security Considerations in System Development Life Cycle (SDLC)	12
2	**Security Threats, Attacks, and Secure Development:** The Need for Security in Modern Systems, Categories of Threats and Attacks (Malware, Phishing, Spoofing, DoS), Social Engineering and Insider Threats, Email Security: Risks, Spoofing, and Secure Email Practices, Secure Software Development Life Cycle (SSDLC), Introduction to Security Policies and Risk Management	12
3	**Cryptography and Cryptanalysis:** Basics of Cryptography, Plaintext & Ciphertext, Cipher Methods, Symmetric Key Cryptography (DES, AES), Asymmetric Key Cryptography (RSA, ECC), Cryptographic Tools and Protocols, Key Management and Digital Signatures, Attacks on Cryptosystems (Brute Force, Cryptanalysis, Side-Channel Attacks)	12

4	**Internet Security Standards and Authentication Mechanisms:** Fundamentals of Internet Standards, Physical and Network Security Fundamentals, Introduction to Authentication, Password-based Authentication, Token and Certificate-Based Authentication, Wireless Network Authentication (WPA, WPA2, WPA3), Authentication Challenges in Mobile and IoT Devices	12
5	**Security Technologies and Infrastructure Protection:** Access Control Mechanisms (DAC, MAC, RBAC), Firewall Types (Packet Filtering, Stateful Inspection, Proxy Firewalls), Virtual Private Networks (VPNs), Securing Remote Access (VPNs, RDP, SSH), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Current Trends in Security Technologies (Zero Trust, SIEM)	12

Practical Content:	

Reference Books:	
1	Introduction to Computer Security by Michael T. Goodrich and Roberto Tamassia, 1st Edition, Published by Pearson, 2010.
2	Principles of Information Security by Michael E. Whitman and Herbert J. Mattord, Fourth Edition, Published by Cengage Learning, 2011.
3	Information Systems Security: Security Management, Metrics, Frameworks and Best Practices by Nina Godbole, Second Edition, Published by Wiley India Pvt. Ltd., 2017.

Web Reference:	
1	https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
2	https://www.eccu.edu/blog/cybersecurity/fundamentals-of-information-security/
3	https://www.classcentral.com/course/swayam-fundamentals-of-information-technology-380848

MOOC/Certificate Course:	
1	https://www.coursera.org/learn/networks-and-network-security
2	https://onlinecourses.swayam2.ac.in/nou25_cs24/preview
3	https://nptel.ac.in/courses/106106157
4	https://www.coursera.org/specializations/cybersecurity-attack-and-defense

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.