Cyber Security
[As per Choice Based Credit System (CBCS) Scheme]
(Effective from the Academic Year 2021-22)
As Per NEP 2020

SEMESTER – V

Course Code	**21BCA56**	CIE Marks	50
Number of Lecture Hours/Week	04	SEE Marks	50
Total Number of Lecture Hours	42	Exam Hours	03

CREDITS-02

Course Objectives:

- Learn the foundations of Cyber security and threat landscape.
- To equip students with the technical knowledge and skills needed to protect and defend against cyber threats.
- To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.
- To expose students to governance, regulatory, legal, economic, environmental, social and ethical contexts of cyber security.
- To expose students to responsible use of online social media networks.

Revised Bloom's Taxonomy Levels: L1 – Remembering, L2 – Understanding, L3 – Applying, L4 – Analyzing, L5 – Evaluating, and L6 – Creating.

Module 1	**Teaching Hours**	**RBT Levels**
Introduction to Cyber crime: Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cyber criminals?, Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime. **Cyber offenses:** How Criminals Plan Them: How Criminals Plan the Attacks, Social Engineering, Cybers talking, Cyber cafe and Cybercrimes, Botnets: The Fuel for Cybercrime.	10	L1,L2, L3,L4, L5
Module 2		
Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.	08	L1,L2, L3,L4, L5

Module 3		
Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft)	08	L1,L2, L3,L4, L5
Module 4		
Understanding Computer Forensics: Introduction, Historical Background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Antiforensics.	08	L1,L2, L3,L4, L5
Module 5		
Cyber Security: Organizational Implications. Introduction, Cost of Cybercrimes and IPR Issues, Web Threats for Organizations, Security and Privacy Implications from cloud computing, Social Media Marketing, Social Computing and the Associated Challenges for Organizations, Protecting People's Privacy in the Organization, Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer Usage Policy.	08	L1,L2, L3,L4, L5

On successful completion of the course, the students will be able to.

CO 1: Understanding about cyber security and cybercrime.
CO 2: Understanding Security Challenges Frauds in Mobile and Wireless Computing.
CO 3: Students are able to Understand tools and methods used in cybercrime.
CO 4: Analyze and evaluate the digital payment system using different techniques.
CO 5: Students are able to get cybercrime and IPR issues.

Question Paper Pattern

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module.
The students will have to answer 5 full questions, selecting one full question from each module..

Text Books:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.(First Edition,2011)
2. Cyber Crime Impact in the New Millennium, by R.C Mishra, Auther Press. Edition2010.
3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson, 13th November,2001).
4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5. Fundamentals of Network Security by E. Maiwald, McGraw Hill.

Reference books:

1. Roger S. Pressman: Software Engineering-A Practitioners approach, 7th edition, Tata McGraw Hill.
2. Pankaj Jalote: An Integrated Approach to software Engineering, Wiley India