PO	1	2	3	4	5	6	7	8	9	10	11	12
Level						M		M				

Syllabus for B. Tech. IV Year I semester
Computer Science and Engineering

CYBER SECURITY

(Mandatory Course)

Code: 7FC20	L	T	P	C
	2	-	-	0

Prerequisite : Nil

Course Objectives:

- To familiarize with network security, network security threats, security services, and countermeasures.
- To be aware of computer security and Internet security.
- To study the defensive techniques against these attacks.
- To familiarize with cyber forensics.
- To be aware of cyber crime related to mobile and laptop etc.
- To acquire knowledge relating to Cyberspace laws and Cyber crimes.
- To understand ethical laws of computer for different countries, Offences under the Cyberspace and Internet in India.

Course Outcomes: At the end of this course the student will be able to

1. Understand cyber-attacks, types of cybercrimes.
2. Realize the importance of cyber security and various forms of cyber attacks and countermeasures.
3. Get familiarity of cyber forensics.
4. Get familiar with obscenity and pornography in cyber space and understand the violation of Right of privacy on Internet.
5. Appraise Cyber laws and also how to protect them self and ultimately the entire Internet community from such attacks.
6. Elucidate the various chapters of the IT Act 2008, power of Central and State Government to make rules under IT Act 2008.

UNIT-I: Introduction to cyber Security

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defense, Security Models, risk management, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc.,

UNIT-II: Cyber Forensics:

Introduction to cyber forensic, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics, Special Techniques for Forensics Auditing.

UNIT-III: 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 and desktop.

UNIT-IV: Cyber Security: Organizational Implications:

Introduction cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations.

Cybercrime and Cyber terrorism: Introduction, intellectual property in the cyberspace, the ethical dimension of cybercrimes the psychology, mindset and skills of hackers and other cyber criminals.

UNIT-V: Privacy Issues:

Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc.

UNIT-VI: Cyberspace and the Law &Miscellaneous provisions of IT Act.

Introduction to Cyber Security Regulations, International Law. The INDIAN Cyberspace, National Cyber Security Policy. Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threats.

Other offences under the Information Technology Act in India, The role of Electronic Evidence and miscellaneous provisions of the IT Act.2008.

Cybercrime: Examples and Mini-Cases

Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.

REFERENCE BOOKS:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&F Group.
3. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2ndEdition, O’ Reilly Media, 2006.
4. Wenbo Mao, “Modern Cryptography – Theory and Practice”, Pearson Education, New Delhi, 2006.