Course Code	Course Title	L	T	P	C
BITE413L	Cyber Security	3	0	0	3
Pre-requisite	NIL	Syllabus version			
		1.0			

Course Objectives:

1. To learn the fundamentals of the cybersecurity domain and related issues
2. To acquire practical knowledge of various tools, processes and methods to ensure security of cyber systems
3. To learn the foundational skills and knowledge of impact of security on legal, business, warfare and social domains

Course Outcomes:

1. Analyze the importance of cybersecurity and cybercrime
2. Recommend the importance of mobile and wireless device security
3. Infer the tools and methods used for cybercrime
4. Summarize the importance of computer forensics and legal perspectives of cybercrimes and cybersecurity
5. Engage awareness on cybercrime and cyber terrorism in social, political, ethical and psychological Dimensions, forensics analysis using hand-held devices

Module:1	Cybercrime and Cyber Terrorism	6 hours

Cybercrime: Definition – Classification of Cybercrimes – Global Perspective on Cybercrimes – Cyberoffenses: How Criminals Plan the Attacks – Social Engineering – Cybertalking – Botnets – Attack Vector - Intellectual Property in the Cyberspace – Copyright – Patent – Trademarks – Trade Secret – Trade Name – The Ethical Dimension of Cybercrimes – Ethical Hackers – Sociology of Cybercriminals – Information Warfare.

Module:2	Security Challenges: Mobile and Wireless Devices	6 hours

Trends in Mobility – Credit Card Frauds in Mobile and Wireless Computing Era – Security Challenges Posed by Mobile Devices – Attacks on Mobile/Cell Phones – Mobile Devices: Security Implications for Organizations – Organizational Measures for Handling Mobile Devices Related Security Issues – Organizational Security Policies and Measures in Mobile Computing Era.

Module:3	Tools and Methods used in Cybercrime	6 hours

Proxy Servers and Anonymizers – Phishing – Password Cracking – Keyloggers and Spywares – Virus and Worms – Trojan Horses and Backdoors – Steganography – DoS and DDoS Attacks – SQL Injection – Buffer Overflow.

Module:4	Cybercrimes and Cybersecurity: The Legal Perspectives	6 hours

Cybercrime and the Legal Landscape around the World – Cyberlaws: The Indian Context – The Indian IT Act – Challenges to Indian Law and Cybercrime Scenario in India – Consequences of not Addressing the Weakness in Information Technology Act – Amendments to the Indian IT Act – Cybercrime and Punishment.

Module:5	**Understanding Computer Forensics**	**6 hours**
Historical Background of Computer Forensics – Digital Forensics Science – The Need for Computer Forensics – Cyberforensics and Digital Evidence – Forensics analysis of E-Mail – Digital Forensics Life Cycle – Network Forensics – Approaching a Computer Forensics Investigation – Relevance of the OSI 7 Layer Model to Computer Forensics – Challenges in Computer Forensics – Special Tools and Techniques – Forensics Auditing – Antiforensics.		
Module:6	**Forensics of Hand-Held Devices**	**7 hours**
Toolkits for Hand-Held Device Forensics – Forensics of iPods and Digital Music Devices – An Illustration on Real Life use of Forensics – Techno Legal Challenges with Evidence from Hand-Held Devices – Organizational Guidelines on Cell Phone Forensics.		
Module:7	**Cybersecurity: Organizational Implications**	**6 hours**
Web Threats for Organizations – Security and Privacy Implications for Cloud Computing – Social Media Marketing – Social Computing and the Associated Challenges for Organizations – Protecting People's Privacy in the Organizations – Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer usage Policy – Media and Asset Protection – Importance of Endpoint Security in Organizations.		
Module:8	**Contemporary Issues**	**2 hours**
	Total Lecture hours:	**45 hours**

Text Book	
1.	"Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, Wiley, 2018.
Reference Books	
1.	"Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives" by Nina Godbole, Sunit Belapure, Wiley, 2011.
2.	Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, Security in Computing, Fifth Edition, Pearson Publishers, 2015.

Mode of Evaluation: Continuous Assessment Tests, Assignment, Quiz, Final Assessment Test			
Recommended by Board of Studies	12-10-2022		
Approved by Academic Council	No. 68	Date	19-12-2022