CYBER SECURITY

IV Semester: MBA								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
CMBC58	**Elective**	4	-	-	4	30	70	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		

I. COURSE OVERVIEW:

This course will learn and gain knowledge about cybercrime, tools and methods used in cybercrime, understanding computer forensic, forensic of hand, cyber security will help to apply it in practical life and in profession life and help to control cybercrimes.

II. COURSE OBJECTIVES:

The students will try to learn:

I. About devices and measurement for handling mobile security policies.
II. Cybercrime tools and methods used in cybercrime and cyber security.
III. The computer forensic system and cyber security.
IV. The technologic challenges from hand held devices.
V. Intellectual property rights for cyber security.

III. COURSE OUTCOMES:

After successful completion of the course, students will be able to:

CO 1: Apply mobile and wireless devices and authentication service security knowledge to protect the safety of authentication.
CO 2: Ensure the security implication for organization and evaluate the handling of mobile security policies in protection of organization.
CO 3: Apply the proxy servers and anonymizers, key loggers and spy wares, virus and worms such tools and methods implement to control cybercrime.
CO 4: Examine the Trojan horse and backdoors and structured query language is applicable to reduce the attacks in cybercrime.
CO 5: Explain the background of cyber forensic and analysis of email and digital forensic life cycle to have computer based knowledge.
CO 6: Evaluate the computer forensic and relevance model to computer forensic for identifying the cybercrime.
CO 7: Verify the cell phone working characteristics and all devices application to find the result.
CO 8: Analyze the technologic challenges with evidence from hand held devices to apply in present technological world.
CO 9: Summarize the intellectual property rights and analyze the web threats for organizations for protection of organization.
CO 10: Evaluate the security and privacy implication and protecting people privacy and implementing it in the organization.

IV. SYLLABUS

UNIT-I	**CYBER CRIME**	**Classes: 08**

Mobile and wireless devices, trend mobility, authentication service security, attacks on mobile phones, mobile phone security implications for organizations, organizational measurement for handling mobile-security policies and measures in mobile computing era.

UNIT-II	**TOOLS AND METHODS USED IN CYBER CRIME**	**Classes: 10**

Proxy servers and Anonymizers, phishing, password cracking, key loggers and spy wares, virus and worms, Trojan horse and backdoors, steganography ,structured query language injection, buffer overflow,attacks on wireless network.

UNIT-III	UNDERSTANDING COMPUTER FORENSIC	Classes: 09
Historical background of cyber forensic, forensic analysis of Email, digital forensic life cycle, network forensic. Setting up a computer forensic laboratory, relevance of the OSI 7 layer model to computer forensic, computer forensic from compliance perspectives.		
UNIT-IV	**FORENSIC OF HAND**	**Classes: 09**
Held devices, understanding cell phone working characteristics, hand-held devices and digital forensic,toolkits for hand-held device, forensic of I pod and digital music devices, technologic challenges with evidence from hand held devices.		
UNIT-V	**CYBER SECURITY**	**Classes:09**
Organizational implications cost of cybercrimes and intellectual property rights issues, web threats for organizations: The evils and perils, social media marketing, security and privacy implications, protecting people privacy in the organizations, forensic best practices for organizations.		

Text Books

1. Dr Mansur Hasib, "Cybersecurity Leadership: Powering the Modern Organization", 2021.
2. Matthew Hickey, "Hands on Hacking: Become an Expert at Next Gen Penetration Testing", 4th Edition, 2020.
3. Kim Crawley, "8 Steps to Better Security a Simple Cyber Resilience Guide for Business", 2020.
4. Paul D. Williams, Matt McDonald "Introduction to Security Studies", 3rd Edition, 2018.
5. Kuan-Ching Li, Brij B. Gupta, Dharma P. Agrawal, "Systems", 2018.
6. Nina Godbole and Sunit Belapure, "Cyber Security", Wiley India, 3rd Edition, 2012.
7. Harish Chander, "Cyber Laws and IT Protection", PHI learning pvt.ltd, 3rd Edition, 2012.
8. Dhiren R Patel, "Information Security Theory and Practice, PHI learning Pvt Ltd, 4th Edition, 2010.

Reference Books:

1. MS.M.K.Geetha and Ms. Swapne Raman" Cyber Crimes and Fraud Management" MacMillan,2012.
2. Pankaj Agrawal, "Information Security and Cyber Laws (Acme Learning)", Excel,2015.
3. VivekSood, "Cyber Law Simplified", TMH,2012.

Web References:

1. https://www.goo.gl/gBUrvc
2. https://www.goo.gl/9Nahvr

E-Text Books:

1. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
2. https://transition.fcc.gov/cyber/cyberplanner.pdf
3. https://www.amazon.in/dp/B07YG4QSZR/ref=cm_sw_r_apan_glt_2FGRNQAEBE4AEV5JQRB7?_encoding=UTF8&psc=1.
4. https://www.amazon.in/dp/B084RH7JNC/ref=cm_sw_r_apan_glt_XSZ2G0M4SF8VE5G45NN5?_encoding=UTF8&psc=1.