COIURE CONTENT

CYBER SECURITY								
IV Semester: MBA								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
CMBD55	**Elective**	4	-	-	4	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisite: Business Analytics								

I. COURSE OVERVIEW:

The aim of this course is to enhance understanding of cyber threats, tools, forensic analysis, and security measures. Participants will gain insights into the vulnerabilities of mobile devices, tools used in cybercrime, computer forensic techniques, and the implications of cyber threats on organizations. The course also covers the forensic analysis of handheld devices and cybersecurity measures to safeguard organizational assets and intellectual property.

II.OBJECTIVES:

The students will try to learn:

I. The cybercrime tools and methods used in cybercrime and cyber security.
II. The computer forensic system and cyber security.
III. Be aware of intellectual property rights for cyber security.
IV. The technologic challenges from hand held devices.

III. COURSE OUTCOMES:

At the end of the course students should be able to:

CO1 Explains the vulnerabilities of mobile and wireless devices, authentication service security, and security implications for organizations.
CO2 Examine proxy servers, phishing, password cracking, malware, and various cyber-attack methods.
CO3 Discuss the historical background of cyber forensic, forensic analysis of email, and the digital forensic life cycle.
CO4 Explore network forensic and the setup of a computer forensic laboratory.
CO5 Illuminate the working characteristics of cell phones, digital forensic for handheld devices, and toolkits for forensic analysis.
CO6 Demonstrate the organizational implications, costs of cybercrimes, intellectual property rights issues, and web threats.

IV. COURSE CONTENT:

MODULE-I-CYBER CRIME (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.

MODULE -II-TOOLS AND METHODS USED IN CYBER CRIME (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.

MODULE -III-UNDERSTANDING COMPUTER FORENSIC (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.

MODULE -IV-FORENSIC OF HAND (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.

MODULE -V-CYBER SECURITY (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.

V. TEXT BOOKS:

1. Dr Mansur Hasib, “Cyber security Leadership: Powering the Modern Organization “, 2021.
2. Matthew Hickey, “Hands on Hacking: Become an Expert at Next Gen Penetration Testing”, 4th edition in 2020.
3. Kim Crawley, “8 Steps to Better Security a Simple Cyber Resilience Guide for Business” in 2020.
4. Paul D. Williams, Matt McDonald “Introduction to Security Studies”3rd edition in 2018.
5. Kuan-Ching Li, Brij B. Gupta, Dharma P. Agrawal “Systems”, in 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.

VI. 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. Vivek Sood, “Cyber Law Simplified”, TMH, 2012

VII. 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.