Savitribai Phule Pune University (Formerly University of Pune)

Board of Studies,
Department of Technology

Electronics & Electrical (EE) Technology

Curriculum Structure for

Professional Certification Programme in Mastering Information Security

Course Name: Professional Certification Programme in Mastering Information Security

Compulsory Modules – 8

Duration: 160 Hours (6 Months)

Course Intake: - 30

Course Mode: - Class Room (Hybrid)

Eligibility Criteria: Graduate from Any Discipline.
Students in penultimate year of graduation or pursuing graduationin any field can also apply.
Working professionals & law enforcement personnel.

Course Contents-					
Sr. No.	**Subject Code**	**Subject Name**	**Credits**	**Teaching Scheme (Theory)**	**Teaching Scheme (Practical)**
1	CPMIS1	Computer & Internet Fundamentals	2	√	√
2	CPMIS2	Understanding the Internet & Network	2	√	
3	CPMIS3	(a) Fundamentals of Cyber Crime, Cyber Security & Hacker Methodologies & Acquisition & (b) Investigation of Digital Evidence	2	√	√
4	CPMIS4	Cyber Forensics & Cyber Crime Investigation	2	√	√
5	CPMIS5	Ethical Wireless Hacking	2	√	
6	CPMIS6	Encryptions & Cryptography	2	√	
7	CPMIS7	Dark Web the Complete Understanding	2	√	
8	CPMIS8	Final Independent Research Project (Dissertation Submission)	6		
		Total Course Credits	**20**		

TAKE AWAY'S AFTER COMPLETION OF (M I S) COURSE

Students develop a thorough detail understanding of how the Cyber world works. They get to know all the important aspects of this virtual world & how to secure the digital environment. After completion of the course students are able to work in various jobs offered in Cyber Security within IT industry. They can also work in Cyber Security Auditing field ensuring safety & protection of digital assets. Students will also gain complete knowledge of digital forensics & how it is conducted using various tools. Students also learn how to draft frameworks, policies & implement them. Students will also be able to demonstrate how to handle security breach incidences & how to implement counter measures.

CPMIS1 Introduction to the Computer hardware, peripherals & Internet Fundamentals

Learning Outcomes

Students will have in-depth knowledge of computers, its components, systems & devices. They will also learn how World Wide Web works & performs all its actions.

Syllabus

The Basics, Internal Components, External Components, System Care and Troubleshooting

Reference:

1. PC Hardware: A Beginner's Guide RON GILSTER
2. The Step-by-step Guide to Understanding Computers By Kevin Wilson
3. COMPUTER ARCHITECTURE : FUNDAMENTALS AND PRINCIPLES OF COMPUTER DESIGN, SECOND EDITION by Joseph D. Dumas II
4. Principles of Computer Hardware by Clements
5. Introduction Computer Hardware Data Comm by Goupille (Author)

CPMIS2 Understanding the Internet & Network

Learning Outcomes

Students will understand the broad concept of internet all of its terminologies, topologies, protocols & functioning. They will also gain knowledge about networking & its significance in real world.

Syllabus

Connecting to the Internet, Exchanging E-mail, Chatting and Conferencing on the Internet, Viewing the World Wide Web, Creating and Maintaining Web Sites, File Transfer and Downloading, Other Internet Topics

Reference:

1. Internet: The Complete Reference, Millennium Edition Margaret Levine Young
2. The Internet Complete Reference by Harley Hahn
3. Fundamentals of The Internet And The World Wide Web Ellen Hepp Reaymond Green law
4. Internet And World Wide Web Simplified by Maran Graphics
5. Internet & World Wide Web: How to Program: International Edition 5th Edition, by Harvey M. Deitel (Author), Paul Deitel (Author), Abbey Deitel (Author)
6. Complete Book of the Internet and World Wide Web (Usborne Computer Guides) by Philippa Wingate (Author), Asha Kalbag (Author), Andy Griffin (Author)

CPMIS 3 (a) Fundamentals of Cyber Crime, Cyber Security & Hacker Methodologies

Learning Outcomes

Students will develop complete understanding about cybercrimes. Various types, terminologies & methods of cybercrimes. How it all functions & propagate along the internet.

Syllabus

Understanding How Hackers & Cyber Criminals work, Web Hacking, E-Mail Hacking, Spoofing Attacks, Computer Worms & Computer Trojans, Computer Viruses

Reference:

1. Mastering Information Security Acquisition & Investigation of Digital Evidence Essential Guide for CCI , CERT, DFIR,CSA,CSE By Transcendental Technologies
2. Cyber Crimes and Cyber Security (GTU)
3. Introduction to Cyber Security : Guide to the World of Cyber Security by Anand Shinde
4. Beginners Guide To Ethical Hacking and Cyber Security by Abhinav Ojha

CPMIS 03 (b) Acquisition & Investigation of Digital Evidence

Learning Outcomes

Students will learn in detail about cyber security incidence breaches. How to investigate cyber crimes & ways to prevent security breaches. Students develop a complete understanding of how to prevent, detect, investigate & report incidences & security breaches.

Syllabus

Introduction, Understanding Networks, Foot-printing & Reconnaissance, Google Hacking, Scanning, System Hacking, Android & I-phone Hacking, Malwares, SQL Injection, Cross Site Scripting, Sniffing, Social Engineering, Identity Theft Fraud, DoS, Session Hijacking, Penetration Testing ,Exploit Writing & Buffer Overflow, Cryptography & Steganography, Firewall & Honeypots, IDS & IPS, Hacking Web Server, Wireless Hacking, Physical Security, Reverse Engineering-Mail Hacking, Security, Compliance & Auditing Incident Handling & Counter Majors

Reference:

1. Mastering Information Security Acquisition & Investigation of Digital Evidence Essential Guide for CCI , CERT, DFIR,CSA,CSE By Transcendental Technologies
2. ASCL Cyber Crime Investigation Manual
3. Blackstone's Handbook of Cyber Crime Investigation by Andrew Staniforth (Author), Police National Legal Database (PNLD) (Author), Professor Babak Akhgar (Author), Francesca Bosco (Author)
4. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors by Anthony Reyes (Author), Richard Brittson (Author), Kevin O'Shea (Author), James Steele (Author)
5. Cyber Crime Investigator's Field Guide by Bruce Middleton (Author)
6. Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition By Albert Marcella, Jr., Doug Menendez

CPMIS4 Cyber Forensics & Cyber Crime Investigation

Learning Outcomes

Students develop a thorough understanding of how to collect & present digital forensic evidence. They learn various tools & software's used to conduct Digital forensics & how to present the same in the court of law.

Syllabus

Introduction, Computer Forensics, Forensic Examination of Digital Evidence, Internet Fraud, Memory Forensics

Reference:

1. Cyber Forensics & Cyber Crime Investigation By Transcendental Technologies
2. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes by Albert Marcella Jr. (Editor), Robert S. Greenfield (Editor)
3. Cyber and Digital Forensic Investigations: A Law Enforcement Practitioner's Perspective: 74 (Studies in Big Data) by Kim-Kwang Raymond Choo (Editor), Nhien-An Le-Khac (Editor)
4. Digital Forensics and Cyber Crime by Daryl Johnson (Editor), Makan Pourzandi (Editor), Pavel Gladyshev (Editor), Sanjay Goel (Editor), Suryadipta Majumdar (Editor)
5. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives (Advances in Digital Crime, Forensics, and Cyber Terrorism) by Raghu Santanam

CPMIS5 Ethical Wireless Hacking

Learning Outcomes

Students learn about the Wi-Fi networks & how to secure & protect them from being hacked. They develop a complete understanding of how securing & protecting networks from attacks & build strategies to protect networks.

Syllabus

Introduction, Wi-Fi Hacking, How is Wireless Network Secured?, Understanding the Hacking System, Hardware Requirements, Attacking the Network, Attacking the WPA Protected Network, Bridging the Airgap, Cracking

Reference:

1. Ethical Wireless Hacking By Transcendental Technologies
2. Hacking Wireless Networks for Dummies by Kevin Beaver (Author), Peter T. Davis (Author), Devin K. Akin (Foreword)
3. Hacking: Wireless Hacking: 3 by Alex Wagner (Author)

CPMIS6 Encryptions & Cryptography

Learning Outcomes

Students learn about encryption techniques & cryptography. They also learn about digital signatures & different Hash values

Syllabus

The Basics of Cryptography, Classic Cryptology, Modern Cryptology, P.G.P

Reference:

1. Secret History The Story of Cryptology By Craig P. Bauer
2. Secret History: The Story of Cryptology (Chapman & Hall/CRC Cryptography and Network Security Series) by Craig Bauer (Author)
3. Real-World Cryptography by David Wong
4. Introduction to Modern Cryptography (2nd edition) Jonathan Katz and Yehuda Lindell
5. Introduction to Cryptography Sahadeo Padhye, Rajeev A. Sahu, Vishal Saraswat

CPMIS7 Dark Web the Complete Understanding

Learning Outcomes

Students will develop a complete understanding of how Dark web exists & operate on the World Wide Web. How illicit activities & organize crime & terrorists operate in the Dark Net. They will also develop skills to tackle the challenges & handle issues arising from dark web.

Syllabus

Introduction to Cyber Security & Dark Web, Threat landscape in Dark Net, Malicious Dark Net / TOR Network, Malware, Cyber criminal Activities in Dark Web, Evolution of the Web and its Hidden Data,Dark Web Content Analyzing Techniques, Extracting Information from Dark Web contents / LOGS, Dark Web Forensics, Open-Source Intelligence,Immerging trends in the Dark Web & Mitigation Techniques

Reference:

1. Inside the Dark Web by Erdal Ozkaya (Author), Rafiqul Islam (Author)
2. The Dark Web... Mystery Untold Kindle Edition by Prakash Prasad
3. TOR: Access the Dark Net, Stay Anonymous Online and Escape NSA Spying (Darknet,Tor Browsing, Dark Web, Hacking Book 1) by Evan Lane (Author),
4. Dark Web Investigation (Security Informatics and Law Enforcement) by Babak Akhgar (Editor), Marco Gercke (Editor), Stefanos Vrochidis (Editor), Helen Gibson (Editor)