

Course Code	Course Title	L	T	P	C
OLMCA603	Cyber Security	3	1	0	4
Pre-requisite	NIL	Syllabus version			
		1.0			
Course Objectives:					
1. Appraise the current structure of cyber security roles across the DoD enterprise, 2. Study the roles and responsibilities of the relevant organizations. 3. Evaluate the trends and patterns that will determine the future state of cyber security.					
Course Outcomes:					
1. Understand the cyber security threat landscape. 2. Develop a deeper understanding and familiarity with various types of cyberattacks, cybercrimes, vulnerabilities and remedies thereto. 3. Analyse and evaluate existing legal framework and laws on cyber security. 4. Analyse and evaluate the digital payment system security and remedial measures against digital payment frauds. 5. Increase awareness about cyber-attack vectors and safety against cyber-frauds.					
Module:1 Introduction to Cyber security					
Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web technology, Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber security.					
Module:2 Cyber Crime Issues					
Unauthorized Access to Computers, Computer Intrusions, Viruses, and Malicious Code, Internet Hacking and Cracking, Virus and worms, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Password Cracking, Steganography, Key loggers and Spyware, Trojan and backdoors, phishing, DOS and DDOS attack, SQL injection, Buffer Overflow.					
Module:3 Cybercrime and Cyber law					
Classification of cybercrimes, Common cybercrimes- cybercrime targeting computers and mobiles, cybercrime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi , Reporting of cybercrimes, Remedial and mitigation measures, Legal perspective of cybercrime, IT Act 2000 and its amendments, Cybercrime and offences, Organizations dealing with Cybercrime and Cyber security in India, Case studies.					
Module:4 Tools and methods used in cyber crime					
Proxy servers and Anonymizers- Phishing Password cracking- Key loggers and Spy wares-Virus and worms-Trojan Horse and Backdoors-Steganography-SQL Injection - Buffer overflow - Attacks on wireless network.					
Module:5 Understanding computer forensic					
Historical background of cyber forensic - Forensic analysis of e-mail- 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. Cases.					

Module:6 Forensic of Hand –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- Techno legal Challenges with evidence from hand-held Devices. Case study.	
Module:7 Cyber Security–Organizational implications	
Cost of cybercrimes and IPR 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. Case study.	
	Total Lecture hours: 120 hours
Text Book(s)	
1.	Nina Godbole & Sunit Belapure "Cyber Security", Wiley India, 2018.
2.	Sumit Belapure and Nina Godbole, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd.
1.	Books, Charles J., Christopher Grow, Philip Craig, and Donald Short, Cybersecurity essentials, 2018, John Wiley & Sons,
2.	Sammons, John, and Michael Cross. The basics of cyber safety: computer and mobile device safety made easy, 2016, Elsevier.
3.	Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies; Security in Computing, 2015, Pearson Education Inc., Sth Edition.
Mode of Evaluation: Quiz / Assignment / Mid-Term, FAT	
Recommended by Board of Studies	01-11-2023
Approved by Academic Council	No. 72 Date: 13-12-2023