Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSC801	Malware Analysis	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSC801	Malware Analysis	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand the fundamental principles and techniques of malware analysis.
2	To gain knowledge of the different types of malware and their capabilities.
3	To develop skills in identifying and analyzing the behavior of malware.
4	To learn how to use various tools and techniques for malware analysis.
5	To understand the importance of threat intelligence in malware analysis.
6	To learn how to write detailed reports on malware analysis findings.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Identify and classify different types of malware based on their behavior and characteristics.	L1, L2, L3
2	Use various tools and techniques to analyze malware and understand their functions and capabilities.	L1, L2
3	Understand the role of threat intelligence in malware analysis and apply it effectively in their analysis.	L1, L2, L3
4	Analyze and evaluate the impact of malware on systems and networks.	L1, L2, L3, L4
5	Create detailed reports on malware analysis findings and communicate their results effectively to respective audiences.	L1, L2, L4, L6
6	Develop effective countermeasures to prevent and mitigate the impact of malware attacks on systems and networks.	L1, L2, L6

Prerequisite: Operating Systems, Computer Networks & Security, C++ Programming, Computer Architecture.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Operating Systems, Computer Networks & Security, C++ Programming, Computer Architecture.	**02**	
I	Introduction to Malware Analysis	Overview of malware and its impact on cybersecurity. Types of malware (e.g., viruses, worms, trojans, ransomware, etc.). Malware delivery methods (e.g., phishing, social engineering, drive-by downloads, etc.). Malware analysis tools and techniques. Basic concepts of assembly language and programming. Malware attack vectors and propagation techniques. Malware behavior and its impact on systems. The role of malware analysis in cyber security. **Self-learning Topics:** Types of malware and their characteristics, Common infection vectors and malware distribution methods, Basic understanding of computer architecture and operating systems, Familiarization with various security tools and techniques.	**06**	CO1
II	Static Malware Analysis	Understanding the structure of executable files Identifying malware characteristics through file analysis (e.g., header, sections, imports, exports, strings, etc.) Static analysis techniques (e.g., file hashing, signature scanning, YARA rules, etc.) Behavioral analysis through static analysis File format analysis Strings and metadata analysis Disassembly and decompilation Code and data flow analysis Malware signature and pattern identification Malware classification and categorization **Self-learning Topics:** Familiarization with file formats and headers, understanding of assembly language and disassembly techniques, Familiarization with static analysis tools such as IDA Pro, Binary Ninja, and radare2, Techniques for detecting packers, obfuscation, and anti-analysis measures.	**08**	CO2
III	Dynamic Malware Analysis	Introduction to dynamic analysis Setting up a malware analysis lab Dynamic analysis environment setup Techniques for dynamic malware analysis (e.g., monitoring system calls, network traffic analysis, memory analysis, etc.) Behavior analysis through dynamic analysis Malware sandboxing and evasion techniques **Self-learning Topics:** Understanding of debugging concepts and techniques, Familiarization with dynamic analysis tools such as OllyDbg, x64dbg, and WinDbg, Techniques for analyzing network traffic and detecting malicious behavior, Familiarization with sandboxing techniques and virtualization tools.	**06**	CO3
IV	Reverse Engineering for Malware Analysis	Introduction to reverse engineering Assembly language basics Reverse engineering tools and techniques Debugging techniques for malware analysis (e.g., using debuggers, disassemblers, and decompilers) Malware unpacking and code injection techniques. Code analysis techniques (e.g., control flow analysis, data flow analysis, etc.)	**06**	CO4

		Code and data reversing Function identification and analysis Anti-debugging and anti-reversing techniques **Self-learning Topics:** Understanding of reverse engineering concepts and techniques, Familiarization with tools such as Ghidra, Hopper, and Binary Ninja, Techniques for identifying and analyzing code functionality, Familiarization with packer unpacking techniques and obfuscation detection.		
V	Advanced Malware Analysis Techniques	Advanced malware analysis techniques (e.g., sandboxing, hypervisor-based analysis, emulation, etc.) Rootkit, bootkit analysis and detection techniques Advanced code obfuscation techniques and their analysis Analysis of malware targeting specific platforms (e.g., mobile devices, IoT, etc.) Polymorphism and metamorphism Shellcode analysis and exploitation Report writing for malware analysis findings. **Self-learning Topics:** Familiarization with techniques for analyzing kernel-mode malware, understanding of rootkit detection and analysis techniques, Techniques for detecting and analyzing fileless malware, Familiarization with machine learning techniques for malware classification and detection.	**07**	CO5
VI	Latest Trends & Research in Malware Analysis	Emerging threats and attack vectors Advanced malware analysis research and techniques Use of artificial intelligence and machine learning in malware analysis Malware analysis case studies Advanced persistent threats (APTs) Zero-day attacks and vulnerabilities Malware analysis automation and scalability **Self-learning Topics:** Familiarization with the latest malware trends and attacks, understanding of emerging malware threats and their characteristics, Familiarization with the latest research and techniques in malware analysis and detection, Techniques for staying up-to-date with the latest developments in malware analysis and cybersecurity.	**04**	CO6

Textbooks:

1. Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software by Abhishek Singh and Michael Sikorski.
2. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code by Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard
3. Learning Malware analysis, Monnappa K A, June 2018 Publisher(s): Packt Publishing ISBN: 9781788392501

References Books:

1. Malware Data Science: Attack Detection and Attribution by Joshua Saxe and Hillary Sanders
2. Gray Hat Hacking: The Ethical Hacker's Handbook by Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, and Jonathan Ness
3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters
4. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation by Bruce Dang, Alexandre Gazet, and Elias Bachaalany
5. Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, and James M. Aquilina

Online References:

1. Practical Malware Analysis: https://nostarch.com/malware
2. Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/cybersecurity
3. Cyber Security India: https://www.cybersecurityindia.in/

Assessment:

Internal Assessment (IA) for 20 marks:

● IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

● Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**
● **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
● A total of **four questions** needs to be answered.

Subject Code	Subject Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8011	Social & Ethical issues of the Internet	03	--	--	03	--	--	03

Subject Code	Subject Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8011	Social & Ethical Issues of the Internet	20	20	20	80	--	--	--	100

Sr. No.	Course Objectives
The course aims:	
1	To gain insights into the aspects of the internet, including ethical and social activities of online systems and networks.
2	To analyze the legal and regulatory governing activities for intellectual property and plagiarism.
3	To understand the social and ethical implications of the internet on individuals, communities, and society as a whole.
4	To explore the laws governing internet security in India.
5	To understand ethical considerations and responsible behavior required in online interactions to preserve privacy and security.
6	To explore and understand various internet services.

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Develop a commitment towards responsible Internet usage and understand various aspects of the online environment.	L1, L2, L3, L4
2	To apply the knowledge of intellectual property rights (IPR) to ensure ethical conduct in academic and professional activities.	L1, L2, L3
3	Evaluate the impact of secret social media lives on individuals and society.	L1, L2, L3, L4, L5
4	Evaluate the recompense of information technology law in addressing issues of data surveillance and privacy.	L1, L2, L3, L4, L5
5	To identify potential security and privacy issues on the Internet.	L1, L2, L3, L4
6	Use knowledge for various internet technologies and services.	L1, L2. L3

Prerequisite: Internet, Networking, Network topology, protocols, working of Internet, network software and hardware components, connection oriented and connectionless services.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Internet, Networking, Network topology, protocols, working of Internet, network software and hardware components, connection oriented and connectionless services.	**02**	--
I	Introduction	What is Internet Ethics? Definition of Internet Ethics, Internet Ethics for everyone, Ethical rules for computer users, Ethical Perspectives, Ethical commitment on Internet, Ethical Aspects of Information Security and Privacy, Freedom of Speech on the Internet, The ethics of AI, Digital Media Ethics, Meta-Ethics, Censorship and Freedom of Expression, Ethics in Social Networks, Lessons for Improving the Ethics Environment. **Self-learning Topics:** Ten Commandments of Computer Ethics.	**06**	CO1

II	IPR & Plagiarism	**Intellectual Property Rights:** Introduction, Concept and Meaning of IPR, General Principles of IPR, Need for Intellectual Property, Different Categories of IPR Instruments, Importance of IPR in Cyber World, International Law Relating to Cybercrimes, Challenges in IPR: From Indian Perspective, Challenges for IP in Digital Economy, Challenges for IP in E-Commerce **Plagiarism:** Concept of Plagiarism, Types, How to avoid Plagiarism, Best Practices, What, Why, and If, Lack of Authorization— Economic Foundations, Lack of Authorization— Natural or Moral Rights **Self-learning Topics:** Lack of Accreditation—Non infringing Plagiarism	**07**	CO2
III	Impact of Technology on Society	Understanding the concept of social change, Social Issues, Accountability in Computer Systems, Secret Social Media Lives, Digital Divide and Social Inequality, Personalization and the Filter Bubble, Positive & Negative Impacts of technology on society, Changing nature of work due to computer technology, Automation. Meaning of Social Media and Social Networking, Tracing the Origin of Popular Social Media and Social Networking Platforms, Advantages and Disadvantages of Social Media and Social Networking, Crimes on Social Media. **Self-learning Topics:** Investigation of Cybercrimes in India	**06**	CO3
IV	Internet Security & Laws	**Conceptions of Data:** Big Data, Datafication, Dataism and dataveillance (Data Surveillance). Non-Government Surveillance, Government Surveillance, Hacktivism. **Information Technology Law**: A Bird's Eye View, Cyber World vis-a-vis need of Legal Protection, Information Technology Act, 2000: A Beginning, Scope of Information Technology Act, 2000, Applicability of Information Technology Act, 2000, Information Technology Act, 2000: A Snapshot, Information Technology (Amendment) Act, 2008, Recompense of Information Technology Law, Limitation of Information Technology Law. **Self-learning Topics:** Cyber Crime: Landmark Judgements in India, Cyber Laws: Recent Trends	**07**	CO4
V	Intelligent User	Introduction, Perspectives on Privacy: Defining Privacy, Harms and Benefits of Privacy, Information Disclosures: Facebook Tags, Enhanced 911 Services, Rewards or Loyalty Programs, Body Scanners, RFID Tags, Implanted Chips, OnStar, Automobile "Black Boxes", Medical Records, Digital Video Recorders, Cookies and Flash Cookies. Public Information, Public Records. Privacy in relation to the Social Good. Ethical Aspects of Privacy. The Unsecure Internet, Keeping Conversations Confidential, Computer Encryption and Mathematics, Confidential Web Browsing, Secure Remote Desktop **Self-learning Topics:** Digital Literacy for Lifelong Learning, Media Literacy, Addressing online harassment, cyberbullying, and trolling	**07**	CO5
VI	Internet Services	Electronic Mail, The World Wide Web: Browsers, HTML And Web Pages, Social Networking And Personal Publishing, Internet Of Things, Internet Search (Search Engines), Voice And Video Communication, File Transfer And Data Sharing, Remote Desktop, Cloud Services and Types of Cloud Services. Cloud Applications and The Internet of Things. **Self-learning Topics:** A Global Digital Library	**04**	CO6

Textbooks:

1. Douglas E. Comer, "The Internet Book_ Everything You Need to Know about Computer Networking and How the Internet Works" Taylor & Francis, Fifth Edition - 2019
2. Asha Vijay Durafe, Dhanashree Toradmalle, "Intellectual Property Rights" Wiley Publications
3. Harish Chander, Gagandeep Kaur, "Cyber Law and IT Protection" Second Edition, PHI Learning.

References:

1. Kenneth Einar Himma and Herman T. Tavani, "The Handbook of Information and Computer Ethics", Wiley Publications, 2008.
2. "Cyber Crime Law and Practice" The Institute of Company Secretaries of India, 2016
3. Michael J. Quinn, "Ethics for the Information Age" Pearson, Sixth Edition, 2015.

Online References:

1. https://www.geeksforgeeks.org/impact-of-technology-on-society/
2. https://open.umich.edu/find/open-educational-resources/information/si-410-ethics-information-technology

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

- Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8012	IoTs & Embedded Security	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8012	IoTs & Embedded Security	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand the fundamentals of IoTs and embedded systems, including their architecture, components, and communication protocols.
2	To gain knowledge of common security vulnerabilities and threats specific to IoT devices and embedded systems.
3	To develop skills to analyze, assess, and mitigate security risks associated with IoTs and embedded systems.
4	To learn various techniques and tools for securing IoT devices, networks, and communication channels.
5	To explore best practices for designing and implementing secure IoT architectures and protocols.
6	To stay updated with emerging trends, advancements, and challenges in IoT security and embedded systems.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Demonstrate a comprehensive understanding of the concepts, principles, and challenges associated with securing IoTs and embedded systems.	L1, L2, L3
2	Analyze and assess the security vulnerabilities and risks in IoT devices, networks, and protocols, and propose effective countermeasures.	L1, L2, L3, L4
3	Apply various techniques and tools for conducting vulnerability assessments and penetration testing on IoT devices and systems.	L1, L2, L3
4	Design and implement secure architectures and protocols for IoT deployments, considering data security, privacy, and authentication requirements.	L1, L2, L3, L4, L5, L6
5	Evaluate and select appropriate security measures, technologies, and frameworks for mitigating security risks in IoT and embedded systems.	L1, L2. L3, L4, L5
6	Stay updated with the latest advancements and emerging trends in IoT security and apply critical thinking to adapt security strategies to evolving threats.	L1, L2

Prerequisite: Computer Networks, Basic Programming, Operating Systems, Cyber Security Fundamentals.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Computer Networks, Basic Programming, Operating Systems, Cyber Security Fundamentals.	**02**	--
I	Introduction to IoTs and Embedded Systems Security	Definition and characteristics of IoTs Overview of embedded systems and their role in IoTs, Importance of security in IoTs and embedded systems, Common IoT applications and their security implications, Challenges and risks in IoTs and embedded systems security, Introduction to security frameworks and standards for IoTs **Self-learning Topics:** Research current and emerging IoT technologies and applications, investigate real-world examples of IoT security breaches and their impact, Explore IoT security frameworks and standards.	**05**	CO1
II	IoT Device Architecture and Security	IoT device components: sensors, actuators, microcontrollers Secure device provisioning and authentication mechanisms Firmware security: secure boot, firmware updates, and integrity checks, Hardware security measures: tamper resistance, secure elements, trusted platform modules (TPM), Security considerations for IoT gateways and edge devices **Self-learning Topics:** Learn about different types of IoT devices and their architectures, Research secure device provisioning and bootstrapping techniques, Explore hardware-based security measures, such as secure elements and trusted platform modules (TPMs)	**07**	CO2
III	Communication Protocols and Network Security for IoTs	Overview of communication protocols used in IoTs (e.g., MQTT, CoAP, HTTP) IoT network architectures: star, mesh, tree, and hybrid topologies, Security mechanisms for IoT communication: encryption, authentication, access control. Network-level security protocols for IoTs: IPsec, DTLS, TLS Security considerations for wireless IoT networks (e.g., Zigbee, Z-Wave, Wi-Fi) **Self-learning Topics:** Dive deeper into specific IoT communication protocols, investigate security vulnerabilities and attacks related to IoT communication protocols, Research IoT network security technologies	**07**	CO3
IV	Vulnerability Assessment and Penetration Testing for IoTs	Understanding common vulnerabilities in IoT devices and systems, IoT threat modeling: identifying and assessing risks. Techniques for vulnerability assessment in IoT environments Penetration testing methodologies for IoT devices and networks Remediation strategies and best practices for IoT security **Self-learning Topics:** Learn about common vulnerabilities and exploits specific to IoT devices and systems, explore tools and methodologies for conducting vulnerability assessments on IoT devices	**05**	CO4
V	Data Security and Privacy in IoTs	Data security challenges in IoTs: confidentiality, integrity, and availability, Secure data transmission and encryption techniques in IoTs, Privacy considerations in IoT data collection and storage Privacy-enhancing technologies for IoTs: anonymization, pseudonymization Compliance with data protection regulations (e.g., GDPR, CCPA) in IoT deployments **Self-learning Topics:** Study encryption algorithms commonly used in IoT data protection, Investigate privacy-enhancing	**07**	CO5

		technologies like differential privacy and homomorphic encryption. Research legal and regulatory frameworks related to IoT data security and privacy.		
VI	Emerging Trends and Advanced Topics in IoT Security	Blockchain technology for secure and decentralized IoT systems Machine learning and AI-driven security solutions for IoTs Edge computing and fog computing in enhancing IoT security and performance. Security considerations for IoT in critical infrastructures (e.g., healthcare, smart cities) Ethical and social implications of IoT security and privacy **Self-learning Topics:** Explore cutting-edge research papers and publications on IoT security, Investigate the role of blockchain technology in securing IoT systems, Learn about machine learning and AI-driven security solutions for IoT threat detection and mitigation	**06**	CO6

Textbooks:

1. "Internet of Things (A Hands-on-Approach)" by Arshdeep Bahga and Vijay Madisetti
2. "Practical Internet of Things Security" by Brian Russell, Drew Van Duren, and John R. Vacca
3. "Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry" by Maciej Kranz

References Books:

1. "Internet of Things: Principles and Paradigms" edited by Rajkumar Buyya, Amir Vahid Dastjerdi, and Sriram Venugopal
2. "Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations" edited by Fei Hu

Online References:

1. IoT Top 10: https://owasp.org/www-project-iot-top-10/
2. IoT Security Foundation: https://www.iotsecurityfoundation.org/
3. NIST Cybersecurity for IoT Program: https://www.nist.gov/programs-projects/cybersecurity-iot-program
4. IoT Security Resources: https://www.sans.org/iot-security/

Assessment:

Internal Assessment (IA) for 20 marks:

●IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

●Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**

●**Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

●A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8013	**Cognitive Psychology in Cyber Security**	**03**	**--**	**--**	**03**	**--**	**--**	**03**

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8013	**Cognitive Psychology in Cyber Security**	**20**	**20**	**20**	**80**	**--**	**--**	**--**	**100**

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To give an overview of cognitive psychology.
2	To study the properties of human memory in reasoning and decision making.
3	To relate the behavior of human in cyberspace.
4	To identify the role of the brain in cyber psychology.
5	To get familiar with the computing environment from cyber-attacks.
6	To analyze psychology with cyber security case studies.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Define the importance of cognitive psychology.	L1, L2
2	Illustrate the reasoning and decision making for solving the problems.	L1, L2, L3
3	Identify the personality behaviors in cyber-crimes.	L1, L2,
4	Study and analyze the behavior of the brain on social media platforms.	L1, L2, L4
5	Describe the computing environment from cyber-attacks.	L1, L2. L3
6	Analyze the psychology aspects through cyber case studies	L1, L2, L4

Prerequisite: Programming Languages, Computer Networks, and Cyber Security

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
I	Introduction to Cognitive Psychology	Introduction to Cognitive psychology, Cognitive Neuroscience, Structure of Nervous System, Measures in Cognitive Neuroscience, **Self-learning Topics:** cognitive psychology as an experimental science	**6**	CO1
II	Reasoning and Decision Making	Perception, Attention, Pervasiveness of memory – Sensory memory, short term and long-term memory, working of memory system, Problem Solving, Deductive Reasoning, Inductive Reasoning, Making decisions. **Self-learning Topics:** Thought process and problem solving	**7**	CO2
III	Behavioral Cyber Security	Exploring the concept of Cyberspace – Human Information Processor – Population – Cyber security without humans – Cyber security and Personality Psychology – Personality theory and assessment. **Self-learning Topics:** Behavioral biases and their impact on decision-making	**7**	CO3
IV	Cyber Psychology	Brain and Cyber psychology - Brain on the internet – Facebook and Socially networked brain – Media Multitasked brain – Cyber addictions- Cyber psychology of video games, Social Engineering, Online Privacy, Cyberbullying. **Self-learning Topics:** Designing a user-friendly security policies	**7**	CO4
V	Computing Environment from Cyber Attacks	Profiling – Social Engineering – Sweeney Privacy – Understanding hackers – Game. theory application to profiling – Behavioral economics – Fake news – Password meters. **Self-learning Topics:** Case Study on successful social engineering attacks and its impact on society.	**7**	CO5
VI	Case Studies	Addressing DDos Attacks – Ransomware – Facebook —This is your digital life – Fake News concerning corona virus, Hacker case studies, Cyber criminals, Cyber-attacks, Understanding the effect of cybercrime. **Self-learning Topics:** Understanding attacker behavior and motivation. Techniques for detecting and preventing social engineering attacks.	**5**	CO6

Textbooks:

1. Cognitive Psychology: Theory, Process, and Methodology Dawn M. McBride, J. Cooper Cutting, SAGE, 2nd Edition.
2. Behavioral Cybersecurity, Wayne Patterson, Cynthia E. Winston-Proctor, CRC Press, 2020
3. Cyberpsychology and the Brain, Thomas D. Parsons, Cambridge University Press, 2017

References Books:

1. A History of Modern Experimental Psychology: From James and Wundt to Cognitive Science, George Mandler, MIT Press
2. Principles of Information Security, Course Technology, by Michael Whitman, Herbert Mattord, Cengage Learning
3. Attention, Perception and Memory: An Integrated Introduction, Elizabeth Styles, ISBN 9780863776595
4. Cyberpsychology: An Introduction to Human-Computer Interaction, Kent L. Norman, Cambridge University Press, 2017
5. Cyber Psychology, N. Suryanarayana, Sonali Publications, ISBN-10 : 8184112815 ISBN-13 : 978-8184112818

Online References:

1. https://www.nist.gov/cyberframework
2. https://nptel.ac.in/courses/109103134
3. J. McAlaney, L. A. Frumkin and V. Benson, Psychological and Behavioral Examinations in Cyber Security, IGI Global, 2018.
4. C. Johnson, R. Gutzwiller, K. Ferguson-Walter and S. Fugate, "A cyber-relevant table of decision making biases and their definitions," ResearchGate, 2020.
5. https://www.mitre.org/sites/default/files/pdf/12_0499.pdf
6. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur. 2021 Jun;105:102248. doi: 10.1016/j.cose.2021.102248. Epub 2021 Mar 3. PMID: 36540648; PMCID: PMC9755115.

Assessment:

Internal Assessment (IA) for 20 marks:

● IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

● Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**

● **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

● A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8014	Intelligent Forensic	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8014	Intelligent Forensic	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	Discuss the need of AI in Digital Forensics.
2	To understand the history of Digital Forensics.
3	To start a crime investigation based on different parameters.
4	To start a crime investigation based on different parameters.
5	To control, preserve, record, and recover evidence from the scene of an incident.
6	To identify Major AI tools and technology that are currently impacting the field of digital forensics.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Identify application of ML for Digital forensics.	L1, L2
2	Understand and Analyze Forensics as Intelligence Sources.	L1, L2, L4
3	Build Intelligence Features of Forensic Evidence.	L1, L3
4	Build Evidence recovery, processing and Verify the Best Practice Using the Main Forensic Evidence Types	L1.L2, L3
5	Interpret and Investigate the Recovery of Forensic Evidence from the crime scene.	L1, L2, L4
6	Explore the Impact of implementing AI tools, technology and frameworks in digital forensics.	L1, L2, L4

Prerequisite: Artificial Intelligence and Digital forensic.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic of AI and DF	**00**	-
I	Machine Learning Trends for Digital Forensics	**1.1 Introduction** Need of Artificial Intelligence in Digital Forensics, Machine Learning Basics, Machine learning for Digital Forensics. Challenges of AI enabled DF. **1.2 Machine Learning Processes** Data Collection and Preprocessing, Training and Testing Phases **1.3 Applications of Machine Learning Models.** Machine Learning Types: Supervised Machine Learning, Unsupervised Machine Learning, Semi-Supervised Machine Learning, Reinforcement Learning **Self-Learning Topic:** Case Study: Using ML for forensics. Using the TON_IoT, Dataset for Forensics.	**04**	CO1
II	Introducing Forensic Intelligence	**2.1 The Beginnings of a Concept of Forensic Intelligence** Forensic Intelligence: Definition, The Concept of 'Entities' in Police Recording Systems, Access to Forensic Support Resources, Forensic Intelligence in Intelligence-Led Policing, The Origins of Forensic Intelligence, Estimating the Number of Current Offenders **2.2 Police Intelligence Models** Police Intelligence Models and the Language of Intelligence-Led Policing, The Four Levels of Crime Divisions in Crime, COMSTAT, Intelligence Models, Intelligence Assets, Knowledge Assets, System Assets, Forensics as Intelligence Sources The Collection of Forensic Intelligence Police Forensic Business Models **Self-Learning Topic:** A Short History of Forensic Intelligence in the Metropolitan Police, An Early Forensic Intelligence Tool Mark Case Example from the Late 1990s, Forensic Intelligence Development in the Metropolitan Police, 2002–2008.	**8**	CO2
III	The Value of Forensics in Crime Analysis and Intelligence	**3.1 Intelligence Features of Forensic Evidence Types** Linking Cases and Comparative Case Analysis The Different Forms of Case Linking in Criminal, The Values of Forensics in Case Linking Analysis, Receiver Operator Characteristics, Truth and Probability, The Crime Detection and Prosecution Rectangle, Dealing with Forensic Crime Links and Clusters, Footwear Evidence Frequency Evaluation **3.2 Forensic Legacy Data** Legacy Data and the FSS Sexual Assault, Forensic Intelligence Service, Improving the Potential of Legacy Data Use, The Importance of Regular Meetings, The Different Experiences of CSIs and Analysts **Self-Learning Topic:** A Footwear Evidence Persistence Case Example, A Linked Homicide Case Example, A Footwear Mark Cluster Example, A Footwear Mark Cluster Example	**7**	CO3
IV	Forensic Evidence	**4.1 Purposes and Objectives of Crime Scene Examinations**		

	Recovery, Processing, and Best Practice	Inhibitors to Effective Uses of Crime Scene Examinations, Forensic Recoveries in Linking Crimes, and in Contributing to the Production of Intelligence Products, Rights or Not to Obtain or Seize Forensic Material from Offenders **4.2 The Advantages of Databasing and Managing Collections of Forensic Evidence** A Scenes of Crime Field Force Checklist for Effective Management of Forensics, Using Intervention Rates and Forensic Recovery Frequencies in Crime Analysis, Issues around Positive and Negative Management Techniques of Forensic Support, The Issue of Areas Disclosed in Forensic Marks as an Enabler of Forensic Intelligence **4.3 Best Practice in Using the Main Forensic Evidence Types** Automatic Fingerprint Identification Systems and Their Characteristics, The Four Factors at Work in Existing Miss Rates with AFIS, Forensic Strategies to Make the Best Use of AFIS, Fingerprint Laboratory Support **4.4 Using DNA Matches and Crime Scene Links Effectively** An Inhibited DNA Casework Example, DNA Databases and eDNA, Significance of DNA Forensic Crime Scene Intervention and Recovery Rates, Forensic Problem Profiles and the Concept of the Forensic Intelligence Report **Self-Learning Topic:** An Example of Volume Crime Practices Inhibiting a Serious Investigation	**10**	CO4
V	Best Practice in Recovery of Forensic Evidence from Crime Scenes	**5.1 Dealing with Crime Scenes** Crime Scene Examinations of Serious and Volume Crimes, Recovery of Different Types of Evidence such as Footwear Marks, Gelatine Lifters, Dealing with Dental Stone Casts, Marks in Snow, Instrument (Tool) Marks Isomark, Microsil, and Casting Putty Materials **5.2 Other Evidence Types** Ballistics, Manufacturing Marks, Evidential Value of Manufacturing Marks, Physical Fits, Contact Trace Evidence, Glass, Dealing with Suspects, Hair Combings, Paint Evidence **5.3 Miscellaneous Traces** Cosmetics, Oils and Greases, Plastics, Rubbers, and Adhesives, Soil, Safe Ballast, and Building Materials, Metals, Other Noxious Chemicals and Other Substances **Self-Learning Topic:** Case study on recovery of digital evidence such as CD, pen drive, Laptop	**6**	CO5
VI	The impact of automation and artificial intelligence on digital forensics	AI and Automation, Automation in context of DF, use of AI in DF, Framework of intelligent automation in digital forensics, Tools and method of intelligent automation in digital forensic, Potential impact of intelligent automation on digital forensic, Tools: Magnet Axiom, Google Takeout Convertor, X-Ways Forensics. **Self-Learning Topic**: Study AI tools for report writing.	**4**	CO6

Textbooks and References:

1. Digital Forensics in the Era of Artificial Intelligence, Author: Nour Moustafa, Publisher: CRC Press, 2022.
2. Forensic Intelligence **By Robert Milne,1st Edition.**
3. Forensic Biology, Author Richard Li, Publisher: CRC Press,2nd Edition.
4. Genetic Surveillance and Crime Control, Authors: Helena Machado and Rafaela Granja.
5. Predictive Policing and Artificial Intelligence, Author: John McDaniel, Ken Pease,1st Edition,2021

Online References:

1. Digital Forensics in the Era of Artificial Intelligence (ebooks.com)
2. **Forensic Intelligence by Robert Milne (ebook) (ebooks.com)**
3. The impact of automation and artificial intelligence on digital forensics (wiley.com)
4. Intelligence-Led Policing: The New Intelligence Architecture (ojp.gov).
5. How AI can be used in forensic science: Challenges and prospects — DocInsights

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

- Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8021	Advanced Blockchain Technology	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8021	Advanced Blockchain Technology	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To get acquainted with the concept of Blockchain Technology.
2	To understand the concept of Ethereum and Hyperledger.
3	To understand the concepts of Security and Privacy in Blockchain
4	To understand the concepts of Scalability and Interoperability in Blockchain.
5	To understand different tokenization on a blockchain.
6	To study Use cases using Blockchain technology concepts for applications in different domains.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
1	Describe the basic concept of Blockchain Technology	L2
2	Develop applications using various blockchain platforms.	L3
3	Interpret the knowledge of Security and Privacy in Blockchain.	L3
4	Interpret the knowledge of Scalability and Interoperability in Blockchain.	L3
5	Describe and classify different token and tokenization.	L2
6	Analyze the use of Blockchain technology using use cases.	L4

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	**Prerequisite**	Fundamental of Blockchain Technology, Programming Language	**2**	--
I	Introduction of Blockchain Technology	Origin of Blockchain, Blockchain Solution, Components of Blockchain, Block in a Blockchain, The Technology and the Future, Types of Blockchain, Introduction of Consensus, Introduction of Smart Contract Security and Privacy Challenges of Blockchain in General, Performance and Scalability, Identity Management and Authentication, Regulatory Compliance and Assurance **Self-Study:** Bitcoin and Bitcoin Network	**6**	CO 1
II	Ethereum and Hyperledger	**Ethereum:** Ethereum Architecture and components, Keys and addresses, Accounts, Transactions and messages, The EVM, Blocks and blockchain, Nodes and miners, Networks, Introducing Remix IDE, Interacting with the Ethereum blockchain with MetaMask. **Hyperledger:** Projects under Hyperledger, Hyperledger reference architecture, Hyperledger Fabric: Key Concept, Components, Consensus Mechanisms, Transaction Lifecycle; Fabric 2.0 **Self-Study:** Solidity Language, Node.js, Hardhat, Cosmos, Hyperledger Caliper	**11**	CO 2
III	Security and Privacy in Blockchain	**Security** in blockchain, Background and historic attacks, Blockchain layered model, Threats and vulnerabilities at each layer of blockchain, including smart contract security, Blockchain layer security, and security at other layers, how to address them, and best practices, Layer 2 security concerns, Tools and techniques to find vulnerabilities, Models to perform threat analysis. **Privacy** and its types, Layer 0, Layer 1, and Layer 2 protocols for privacy on blockchain, Zero-knowledge proofs, their various types, polynomial commitment schemes, and relevant protocols, Example **Self-Study:** Blockchain Security and Privacy for smart contracts, healthcare systems, IoT, Supply chain, etc.	**7**	CO 3
IV	Scalability and Interoperability in Blockchain	**Scalability:** Blockchain scalability trilemma, Methods to improve blockchain scalability, Layer 0, 1, 2, and beyond **Interoperability:** Blockchain Interoperability, Use Cases, Layers of Blockchain Interoperability, Variations in Blockchain Implementations Characterization of Existing Blockchain Interoperability Approaches. **Self-Study:** Study and Analyze Technical paper related to Scalability and Interoperability in Blockchain Technology	**5**	CO 4
V	Tokenization	Tokenization on a blockchain, Types of tokens, Process of tokenization, Token offerings, Token standards, building an ERC-20 token, Emerging concepts. **Self-learning Topics:** Defi, Types of cryptocurrencies in the market	**3**	CO 5

VI	Use Cases	Web3 Development Using Ethereum, **use cases** including IoT, government, health, and Artificial Intelligence (AI), emerging trends, challenges. **Metaverse:** Introduction to Metaverse, Metaverse layers, Metaverse tokens **Self-learning Topics:** Advanced Applications of Blockchain using Web3.0 in Digital identity, Intellectual Property Protection, Energy trading and Grid Management	**5**	CO 6

Textbooks:

1. S. CHANDRAMOULI, Blockchain Technology. ORIENT BLACKSWAN PVT Limited, 2020.
2. Imran Bashir, Mastering Blockchain - Fourth Edition Packt Publishing.

References - Technical Papers:

1. I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi and P. Szalachowski, "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 341-390, First quarter 2021, doi: 10.1109/COMST.2020.3033665.
2. Bansod, S., Ragha, L. Challenges in making blockchain privacy compliant for the digital world: some measures. Sādhanā 47, 168 (2022). https://doi.org/10.1007/s12046-022-01931-1
3. Kang, Inwon, Aparna Gupta, and Oshani Seneviratne. "Blockchain Interoperability Landscape." arXiv preprint arXiv:2212.09227 (2022).

Online References:

1. https://www.udemy.com/course/metaverse-fundamentals-blockchain-cryptocurrency-and-nfts/
2. "Blockchain Architecture Design And Use Cases", NPTEL: https://nptel.ac.in/courses/106/105/106105184/

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

- Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8022	Metaverse	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8022	Metaverse	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To study the concepts of Metaverse.
2	To study Metaverse and Web 3.0, Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), NFT in Blockchain.
3	To study the Metaverse technologies and protocols.
4	To study and identify the required infrastructure for Metaverse.
5	To Study various case studies of Metaverse.
6	To Study of Metaverse Immersive technology and Interfaces

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Explore the concepts of Metaverse.	L3,L4
2	Describe the fundamental concepts needed for the metaverse.	L1,L2
3	Explain the Metaverse technologies and protocols.	L2,L4
4	Construct the required infrastructure for Metaverse.	L3
5	Describe Metaverse Immersive technology and Interfaces	L1,L2
6	Express the different case studies of Metaverse	L2,L3,L4

Prerequisite: Concepts of Blockchain

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic Concepts of Blockchain Technology.	**01**	-
I	Introduction:	What is the Metaverse? History of metaverse, Evaluation of Technology: Web, AR VR, 3D spaces. Immersive learning, Blockchain, Decentralized commerce, challenges and opportunities of metaverse **Self-learning:** AR VR tools, Blockchain technology	**04**	CO1
II	Fundamental Concepts of Metaverse	Building block technology of metaverse, How Gaming + Web 3.0 + Blockchain are Changing the Internet: Future of Internet. How Metaverse is different from the Internet, Potential of Metaverse, characteristics of metaverse. The Different Shapes of the Metaverse: Games, NFTs (assets), Blockchain Protocols, Cryptocurrencies, etc. **Self-learning:** Case Study on NFT, Cryptocurrency and Blockchain platforms	**08**	CO2
III	Metaverse Technologies and Protocols	Metaverse technologies, principles, affordances and application, Blockchain Protocols and Platforms Involved in the Metaverse, Metaverse-Related Tokens, Blockchain NFT need for metaverse: working principle of blockchain, NFT based virtual assets in metaverse, case study. How NFTs are Unlocking the Metaverse, Potential working of ERC721 NFT	**08**	CO3
IV	Metaverse Infrastructure	Access the metaverse, necessary hardware and Infrastructure, Interface. Understanding Decentraland, native token MANA, creating Avatar. Using metamask to access Decentraland, owning land to have direct access of metaverse	**07**	CO4
V	Metaverse Immersive technology and Interfaces	3d Reconstruction, AI technology to analyses 3D Scan Virtual Reality (VR) and Augmented Reality (AR), Mixed Reality (MR) and Extended Reality (XR), Metaverse vs VR what is difference, IoT to bridge gap between physical world and internet, Metaverse Interfaces: Personal Computer, Mobile Phone, AR Glasses, VR Goggles, Neuralink	**08**	CO5
VI	Case studies of Metaverse:	Various use cases of metaverse, Industries Disrupted by the Metaverse: Fashion, Marketing, Brands, Finance, Gaming, Architecture, Virtual Shows/Concerts, Art Galleries and Museums. Virtual Business and market: Investing in the Metaverse and Profit. Asset Classes Inside the Metaverse. Metaverse Land Ownership - Property Investment	**04**	CO6

Text & Reference Books:

1. Metaverse For Beginners A Guide To Help You Learn About Metaverse, Virtual Reality And Investing In NFTs By Andrew Clemens, 2022.
2. Extended Reality and Metaverse Immersive Technology in Times of Crisis, Springer Proceedings in Business and Economics, International XR Conference 2022.
3. Mystakidis, Stylianos, " Metaverse",Journal=Encyclopedia,2022, https://www.mdpi.com/2673-8392/2/1/31
4. All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda, Technical Report · October 2021

Online References:

1. **https://www.udemy.com/course/complete-metaverse-course-everything-about-ar-vr-and-nft/**

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

- Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8023	Green IT	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
CSDO8023	Green IT	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand what Green IT is and how it can help improve environmental Sustainability.
2	To understand the principles and practices of Green IT.
3	To understand how Green IT is adopted or deployed in enterprises.
4	To understand how data centers, cloud computing, storage systems, software and networks can be made greener.
5	To measure the Maturity of a Sustainable ICT world.
6	To implement the concept of Green IT in Information Assurance in Communication and social media and all other commercial fields.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Describe awareness among stakeholders and promote green agenda and green initiatives in their working environments leading to green movement.	L1
2	Identify IT Infrastructure Management and Green Data Center Metrics for software development	L1, L2
3	Recognize Objectives of Green Network Protocols for Data communication.	L1, L2
4	Use Green IT Strategies and metrics for ICT development.	L1, L2, L3
5	Illustrate various green IT services and its roles	L1, L2
6	Use new career opportunities available in the IT profession, audits and others with special skills such as energy efficiency, ethical IT assets disposal, carbon footprint estimation, reporting and development of green products, applications and services.	L1, L2, L3

Prerequisite: Environmental Studies

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Environmental Studies	**2**	
I	Introduction	Environmental Impacts of IT, Holistic Approach to Greening IT, Green IT Standards and Eco-Labeling, Enterprise Green IT Strategy, Green IT: Burden or Opportunity? Hardware: Life Cycle of a Device or Hardware, Reuse, Recycle and Dispose. Software: Introduction, Energy Saving Software Techniques, Evaluating and Measuring Software Impact to Platform Power. **Self-Learning:** Evaluating and Measuring software impact to platform power	**6**	CO1
II	Software development and data centers	Sustainable Software, Software Sustainability Attributes, Software Sustainability Metrics, Sustainable Software Methodology, Data Centers and Associated Energy Challenges, Data Centre IT Infrastructure, Data Centre Facility Infrastructure: Implications for Energy Efficiency, IT Infrastructure Management, Green Data Centre Metrics **Self-learning Topics:** Sustainable Software: A Case Study, Data Centre Management Strategies	**6**	CO1, CO2
III	Data storage and communication	Storage Media Power Characteristics, Energy Management Techniques for Hard Disks, System-Level Energy Management, Objectives of Green Network Protocols, Green Network Protocols and Standards **Self-learning Topics:** System-Level Energy Management	**6**	CO1, CO3
IV	Information systems, green IT strategy and metrics	Approaching Green IT Strategies, Business Drivers of Green IT Strategy, Business Dimensions for Green IT Transformation, Multilevel Sustainable Information, Sustainability Hierarchy Models, Product Level Information, Individual Level Information, Functional Level Information, Organizational Level Information, Regional/City Level Information, Measuring the Maturity of Sustainable ICT. **Self-learning Topics:** Business Dimensions for Green IT transformation.	**6**	CO1, CO4
V	Green IT services and roles	Factors Driving the Development of Sustainable IT, Sustainable IT Services (SITS), SITS Strategic Framework, Sustainable IT Roadmap, Organizational and Enterprise Greening, Information Systems in Greening Enterprises, Greening the Enterprise: IT Usage and Hardware, Inter-organizational Enterprise Activities and Green Issues, Enablers and Making the Case for IT and the Green Enterprise. **Self-learning Topics:** Inter-organizational Enterprise Activities and Green Issues, Enablers and Making the Case for IT and the Green Enterprise.	**6**	CO1, CO4 CO5
VI	Managing and regulating green IT	Strategizing Green Initiatives, Implementation of Green IT, Information Assurance, Communication and social media, The Regulatory Environment and IT Manufacturers, Nonregulatory Government Initiatives, Industry Associations and Standards Bodies, Green Building Standards, Green Data Centers, Social Movements and Greenpeace. Case study on: Industry Sustainability with Green IT, Managing Green IT, The energy	**7**	CO1, CO5 CO6

		consumption in Torrent systems with malicious content, The use of thin client instead of desktop PC **Self-learning Topics:** Information Assurance, Green Data Centers		

Textbooks:

1. San Murugesan, G. R. Gangadharan, Harnessing Green IT, WILEY 1st Edition-2018
2. Mohammad Dastbaz Colin Pattinson Babak Akhgar, Green Information Technology A Sustainable Approach , Elsevier 2015
3. Reinhold, Carol Baroudi, and Jeffrey Hill Green IT for Dummies, Wiley 2009

References:

1. Mark O'Neil, Green IT for Sustainable Business Practice: An ISEB Foundation Guide, BCS
2. Jae H. Kim, Myung J. Lee Green IT: Technologies and Applications, Springer, ISBN: 978-3-642- 22178-1
3. Elizabeth Rogers, Thomas M. Kostigen the Green Book: The Everyday Guide to Saving the Planet One Simple Step at a Time, Springer

Assessment:

Internal Assessment (IA) for 20 marks:

- IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

- Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **four questions** needs to be answered.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO8024	Cyber Security laws & legal aspects	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
CSDO8024	Cyber Security laws & legal aspects	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	Understand the fundamental concepts and principles of cyber law and its relevance in the digital age.
2	Explore the legal implications of various cybercrimes and develop an understanding of the legal provisions and penalties associated with them.
3	Gain knowledge of the legal aspects of cyber contracts, intellectual property rights, and their enforcement in the digital domain.
4	Comprehend the legal frameworks, regulations, and compliance requirements related to information security in various industries.
5	Examine the ethical and social implications of cyber activities and develop an ethical framework for responsible digital behavior.
6	Analyze and evaluate the legal challenges in cybersecurity incidents and develop strategies for risk management and incident response.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Demonstrate a comprehensive understanding of the principles, concepts, and historical background of cyber law and its application in real-world scenarios.	L1, L2
2	Identify and classify different types of cybercrimes, understand the legal provisions and penalties associated with them, and effectively investigate and prosecute cybercrimes.	L1, L2
3	Evaluate the legal aspects of cyber contracts and intellectual property rights, including their formation, validity, enforceability, and protection in the digital era.	L2, L3
4	Analyze and interpret the legal frameworks, regulations, and compliance requirements related to information security standards in different industries.	L1, L2, L3
5	Recognize and assess the ethical and social implications of cyber activities, and apply ethical frameworks and principles in cybersecurity practices.	L1, L2
6	Develop a comprehensive understanding of the legal challenges in cybersecurity incidents, including incident response, breach notification, liability, and risk management.	L2, L3

Prerequisite: Basic knowledge of computer networks, information technology, and cybersecurity, awareness of the ethical implications of technology and digital activities, critical thinking and analytical skills for legal analysis and evaluation.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic knowledge of computer networks, information technology, and cybersecurity, awareness of the ethical implications of technology and digital activities, critical thinking and analytical skills for legal analysis and evaluation.	**01**	
I	Introduction to Cyber Law and Legal Aspects	• What is Cyber Law? • Need for Cyber Law • Historical background and evolution of cyber law • Key principles and concepts of cyber law • Legal frameworks and regulations related to cybersecurity. • Overview of international cyber law and its relevance • Case studies illustrating the application of cyber law in real-world scenarios. **Self-learning Topics:** Comparative analysis of cyber laws in different countries, Emerging trends and challenges in cyber law, Legal implications of emerging technologies (e.g., artificial intelligence, blockchain), Research and study of landmark cyber law cases	**04**	CO1
II	Legal Implications of Cyber Crimes	• Introduction to Criminal Law • Classification and types of cybercrimes (e.g., hacking, identity theft, cyber fraud) • Legal provisions and penalties for different cybercrimes(Sections based on crimes) • Investigation and prosecution of cybercrimes • Jurisdictional Issues in cybercrime cases • Role of digital evidence in cybercrime investigations • Case studies on high-profile cybercrime incidents and their legal implications **Self-learning Topics:** Study of cybercrime laws in specific jurisdictions, Analysis of cybercrime statistics and trends, Ethical considerations in cybercrime investigations, Legal challenges in cross-border cybercrime cases	**08**	CO2
III	Cyber Contracts and Intellectual Property Rights	• Legal aspects of cyber contracts, including formation, validity, and enforceability • Intellectual property rights in the digital domain (e.g., copyright, trademarks, patents) • Protection and enforcement of intellectual property rights in the digital era • Digital rights management and anti-piracy measures • Emerging issues in cyber contracts and intellectual property rights (e.g., open-source software, digital content licensing) **Self-learning Topics:** Comparative analysis of intellectual property laws in different countries, Study of legal cases involving cyber contracts and intellectual property disputes, Examination of licensing agreements and their legal implications.	**08**	CO2
IV	Concepts of Cyberspace & Cyber Law	• Introduction to e-Commerce • Contract & Security Aspects in Cyber Law • Intellectual Property & Evidence Aspect in Cyber Law • Criminal Aspects in Cyber Law • Need for Indian Cyber Law **Self-learning Topics:** Internet governance models and organizations (e.g., ICANN, ITU), Cyber sovereignty and jurisdictional challenges, Cybersecurity challenges in the digital era	**07**	CO4

V	Information technology Act	• Introduction of Cybercrime • Information Technology Act, 2000 • Offences under IT Act, 2000 • IT Act, 2008 & its Amendments **Self-learning Topics:** Cybercrimes and their classification under the IT Act, Investigation and prosecution of cybercrimes under the IT Act, Role of digital evidence in cybercrime cases.	**08**	CO5
VI	Information Security Standard Compliances	• PCI Compliance • ISO/IEC 27000 • North American Electric Reliability Corporation (NERC) • Health Insurance Portability and Accountability Act (HIPAA) • Sarbanes-Oxley Act (SOX) **Self-learning Topics:** Audit and assessment processes for information security compliance, Incident response and breach notification procedures, Legal considerations in information security governance and compliance	**04**	CO6

Text Books:

1. "Cyber Security & Cyber Laws" by Nilakshi Jain & Ramesh Menon (Unit 4,5,6)
2. "Cyber Law Simplified" by Vivek Sood (Unit 1)
3. "Cyber Crime: Law and Practice" by Pavan Duggal (Unit 2)
4. "Intellectual Property Rights in Cyberspace" by Rajendra Kumar (Unit 3)
5. "Understanding Cyberspace Law" by George B. Delta and Jeffrey H. Matsuura (Unit 4)
6. "Information Technology Law and Practice" by Vakul Sharma (Unit 5)

References Books:

1. "Cyber Law: The Indian Perspective" by Karnika Seth
2. "Cyber Law and Crimes" by Dr. N.K. Aggarwal
3. "Cyber Law, Contracts, and Intellectual Property Rights" by A. Jayanthi
4. "Cyber Law: Indian and International Perspectives" by Yatindra Singh and Shantanu Chattopadhyay
5. "Information Technology Law in India" by Vakul Sharma
6. "Information Security Management: Concepts and Practice" by Prashant Pathak and Sushil Chandra

Online References:

1. Stanford Law School's Center for Internet and Society (https://cyberlaw.stanford.edu/)
2. Electronic Frontier Foundation (EFF) (https://www.eff.org/)
3. National Institute of Standards and Technology (NIST) Cybersecurity Framework (https://www.nist.gov/cyberframework)
4. International Association of Privacy Professionals (IAPP) (https://iapp.org/)
5. United Nations Commission on International Trade Law (UNCITRAL) - Electronic Commerce and Information Technology (https://uncitral.un.org/en/working_groups/6/electronic_commerce)

Assessment:

Internal Assessment (IA) for 20 marks:

● IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of syllabus content must be covered in First IA Test and remaining 40% to 50% of syllabus content must be covered in Second IA Test

Question paper format

● Question Paper will comprise of a total of **six questions each carrying 20 marks.** Q.1 will be **compulsory** and should **cover maximum contents of the syllabus.**

● **Remaining questions** will be **mixed in nature** (part (a) and part (b) of each question must be from different modules. For example, if Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)

● A total of **four questions** needs to be answered.

Subject Code	Subject Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8011	Project Management	03	--	--	03	--	--	03

Subject Code	Subject Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
ILO8011	Project Management	20	20	20	80	--	--	--	100

Course Objectives:

	Course Objectives:
	The course aims:
1	To familiarize the students with the use of a structured methodology/approach for each and every unique project undertaken, including utilizing project management concepts, tools and techniques.
2	To appraise the students with the project management life cycle and make them knowledgeable about the various phases from project initiation through closure

Course Outcomes:

	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Apply selection criteria and select an appropriate project from different options.	L3
2	Write work breakdown structure for a project and develop a schedule based on it.	L1, L6
3	Identify opportunities and threats to the project and decide an approach to deal with them strategically.	L1, L4
4	Use Earned value technique and determined & predict status of the project.	L3, L5
5	Capture lessons learned during project phases and document them for future reference	L3

Module	Detailed Contents	Hrs
01	**Project Management Foundation:** Definition of a project, Project Vs Operations, Necessity of project management, Triple constraints, Project life cycles (typical & atypical) Project phases and stage gate process. Role of project manager. Negotiations and resolving conflicts. Project management in various organization structures. PM knowledge areas as per Project Management Institute (PMI).	5
02	**Initiating Projects:** How to get a project started, selecting projects strategically, Project selection models (Numeric /Scoring Models and Non-numeric models), Project portfolio process, Project sponsor and creating charter; Project proposal. Effective project team, Stages of team development & growth (forming, storming, norming & performing), team dynamics.	6
03	**Project Planning and Scheduling:** Work Breakdown structure (WBS) and linear responsibility chart, Interface Coordination and concurrent engineering, Project cost estimation and budgeting, Top down and bottoms up budgeting, Networking and Scheduling techniques. PERT, CPM, GANTT chart. Introduction to Project Management Information System (PMIS).	8
04	**Planning Projects:** Crashing project time, Resource loading and leveling, Goldratt's critical chain, Project Stakeholders and Communication plan. Risk Management in projects: Risk management planning, Risk identification and risk register. Qualitative and quantitative risk assessment, Probability and impact matrix. Risk response strategies for positive and negative risks	6
05	**Executing Projects:** **5.1 Executing Projects:** Planning monitoring and controlling cycle. Information needs and reporting, engaging with all stakeholders of the projects. Team management, communication and project meetings. **Monitoring and Controlling Projects:** Earned Value Management techniques for measuring value of work completed; Using milestones for measurement; change requests and scope creep. Project audit. **Project Contracting** Project procurement management, contracting and outsourcing,	8
06	**Project Leadership and Ethics:** Introduction to project leadership, ethics in projects. Multicultural and virtual projects. **Closing the Project:** Customer acceptance; Reasons of project termination, Various types of project terminations (Extinction, Addition, Integration, Starvation), Process of project termination, completing a final report; doing a lessons learned analysis; acknowledging successes and failures; Project management templates and other resources; Managing without authority; Areas of further study.	6

References:

1. Jack Meredith & Samuel Mantel, Project Management: A managerial approach, Wiley India, 7thEd.
2. A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 5th Ed,Project Management Institute PA,USA
3. Gido Clements, Project Management, CengageLearning.
4. Gopalan, Project Management, , WileyIndia
5. Dennis Lock, Project Management, Gower Publishing England, 9 thEd.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be a compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:

Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question paper weightage of each module will be proportional to the number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module3)
4. Only Four questions need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8012	Finance Management	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
ILO8012	Finance Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	Overview of Indian financial system, instruments and market
2	Basic concepts of value of money, returns and risks, corporate finance, working capital and its management
3	Knowledge about sources of finance, capital structure, dividend policy

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand Indian finance system and corporate finance	L1
2	Discuss investment, finance as well as dividend decisions	L2

Module	Detailed Contents	Hrs
01	**Overview of Indian Financial System:** Characteristics, Components and Functions of Financial System. **Financial Instruments:** Meaning, Characteristics and Classification of Basic Financial Instruments — Equity Shares, Preference Shares, Bonds-Debentures, Certificates of Deposit, and Treasury Bills. **Financial Markets:** Meaning, Characteristics and Classification of Financial Markets — Capital Market, Money Market and Foreign Currency Market **Financial Institutions:** Meaning, Characteristics and Classification of Financial Institutions — Commercial	06

	Banks, Investment-Merchant Banks and Stock Exchanges	
02	**Concepts of Returns and Risks:** Measurement of Historical Returns and Expected Returns of a Single Security and a Two-security Portfolio; Measurement of Historical Risk and Expected Risk of a Single Security and a Two-security Portfolio. **Time Value of Money:** Future Value of a Lump Sum, Ordinary Annuity, and Annuity Due; Present Value of a Lump Sum, Ordinary Annuity, and Annuity Due; Continuous Compounding and Continuous Discounting.	06
03	**Overview of Corporate Finance:** Objectives of Corporate Finance; Functions of Corporate Finance—Investment Decision, Financing Decision, and Dividend Decision. **Financial Ratio Analysis:** Overview of Financial Statements—Balance Sheet, Profit and Loss Account, and Cash Flow Statement; Purpose of Financial Ratio Analysis; Liquidity Ratios; Efficiency or Activity Ratios; Profitability Ratios. Capital Structure Ratios; Stock Market Ratios; Limitations of Ratio Analysis.	09
04	**Capital Budgeting:** Meaning and Importance of Capital Budgeting; Inputs for Capital Budgeting Decisions; Investment Appraisal Criterion—Accounting Rate of Return, Payback Period, Discounted Payback Period, Net Present Value (NPV), Profitability Index, Internal Rate of Return (IRR), and Modified Internal Rate of Return (MIRR) **Working Capital Management:** Concepts of Meaning Working Capital; Importance of Working Capital Management; Factors Affecting an Entity's Working Capital Needs; Estimation of Working Capital Requirements; Management of Inventories; Management of Receivables; and Management of Cash and Marketable Securities.	10
05	**Sources of Finance:** Long Term Sources—Equity, Debt, and Hybrids; Mezzanine Finance; Sources of Short Term Finance—Trade Credit, Bank Finance, Commercial Paper; Project Finance. **Capital Structure:** Factors Affecting an Entity's Capital Structure; Overview of Capital Structure Theories and Approaches— Net Income Approach, Net Operating Income Approach; Traditional Approach, and Modigliani-Miller Approach. Relation between Capital Structure and Corporate Value; Concept of Optimal Capital Structure	05
06	**Dividend Policy:** Meaning and Importance of Dividend Policy; Factors Affecting an Entity's Dividend Decision; Overview of Dividend Policy Theories and Approaches—Gordon's Approach, Walter's Approach, and Modigliani- Miller Approach	03

REFERENCES:

1. Fundamentals of Financial Management, 13th Edition (2015) by Eugene F. Brigham and Joel F. Houston; Publisher: Cengage Publications, New Delhi.
2. Analysis for Financial Management, 10th Edition (2013) by Robert C. Higgins; Publishers: McGraw Hill Education, New Delhi.
3. Indian Financial System, 9th Edition (2015) by M. Y. Khan; Publisher: McGraw Hill Education, New Delhi.
4. Financial Management, 11th Edition (2015) by I. M. Pandey; Publisher: S. Chand (G/L) & Company Limited, New Delhi.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:
Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question.
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4. Only Four question need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8013	Entrepreneurship Development and Management	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
ILO8013	Entrepreneurship Development and Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To acquaint with entrepreneurship and management of business.
2	Understand Indian environment for entrepreneurship.
3	Idea of EDP,MSME.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand the concept of business plan and ownerships	L1
2	Interpret key regulations and legal aspects of entrepreneurship in India	L5
3	Understand government policies for entrepreneurs.	L1

Module	Detailed Contents	Hrs
01	**Overview Of Entrepreneurship:** Definitions, Roles and Functions/Values of Entrepreneurship, History of Entrepreneurship Development, Role of Entrepreneurship in the National Economy, Functions of an Entrepreneur, Entrepreneurship and Forms of Business Ownership Role of Money and Capital Markets in Entrepreneurial Development: Contribution of Government Agencies in Sourcing information for Entrepreneurship	04
02	**Business Plans And Importance Of Capital To Entrepreneurship:** Preliminary and Marketing Plans, Management and Personnel, Start-up Costs and Financing as well as Projected Financial Statements, Legal Section, Insurance, Suppliers and Risks, Assumptions and Conclusion, Capital and its Importance to the Entrepreneur **Entrepreneurship And Business Development:** Starting a New Business, Buying an Existing Business, New Product Development, Business Growth and the Entrepreneur Law and its Relevance to Business Operations	09
03	Women's Entrepreneurship Development, Social entrepreneurship-role and need, EDP cell, role of sustainability and sustainable development for SMEs, case studies, exercises	05
04	**Indian Environment for Entrepreneurship:** key regulations and legal aspects , MSMED Act 2006 and its implications, schemes and policies of the Ministry of MSME, role and responsibilities of various government organisations, departments, banks etc., Role of State governments in terms of infrastructure developments and support etc., Public private partnerships, National Skill development Mission, Credit Guarantee Fund, PMEGP, discussions, group exercises etc	08
05	**Effective Management of Business:** Issues and problems faced by micro and small enterprises and effective management of M and S enterprises (risk management, credit availability, technology innovation, supply chain management, linkage with large industries), exercises, e-Marketing	08
06	**Achieving Success In The Small Business:** Stages of the small business life cycle, four types of firm-level growth strategies, Options – harvesting or closing small business Critical Success factors of small business	05

REFERENCES:

1. Poornima Charantimath, Entrepreneurship development- Small Business Enterprise, Pearson
2. Education Robert D Hisrich, Michael P Peters, Dean A Shapherd, Entrepreneurship, latest edition, The McGrawHill Company
3. Dr TN Chhabra, Entrepreneurship Development, Sun India Publications, New Delhi
4. Dr CN Prasad, Small and Medium Enterprises in Global Perspective, New century Publications, New Delhi
5. Vasant Desai, Entrepreneurial development and management, Himalaya Publishing House
6. Maddhurima Lall, Shikah Sahai, Entrepreneurship, Excel Books
7. Rashmi Bansal, STAY hungry STAY foolish, CIIE, IIM Ahmedabad
8. Law and Practice relating to Micro, Small and Medium enterprises, Taxmann Publication Ltd.
9. Kurakto, Entrepreneurship- Principles and Practices, Thomson Publication
10. Laghu Udyog Samachar
11. www.msme.gov.in
12. www.dcmesme.gov.in
13. www.msmetraining.gov.in

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:
Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4. Only Four question need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8014	Human Resource Management	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
ILO8014	Human Resource Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To introduce the students with basic concepts, techniques and practices of human resource management.
2	To provide an opportunity of learning Human resource management (HRM) processes, related with the functions, and challenges in the emerging perspective of today's organizations.
3	To familiarize the students about the latest developments, trends & different aspects of HRM.
4	To acquaint the student with the importance of interpersonal & inter-group behavioral skills in an organizational setting required for future stable engineers, leaders and managers.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand the concepts, aspects, techniques and practices of human resource management.	L1
2	Understand the Human resource management (HRM) processes, functions, changes and challenges in today's emerging organizational perspective.	L1
3	Gain knowledge about the latest developments and trends inHRM.	L1, L6
4	Apply the knowledge of behavioral skills learnt and integrate it within an interpersonal and intergroup environment emerging as future stable engineers and managers.	L3

Module	Detailed Contents	Hrs
01	**Introduction to HR** • Human Resource Management- Concept, Scope and Importance, Interdisciplinary Approach Relationship with other Sciences, Competencies of HR Manager, HRM functions. • Human resource development (HRD): changing role of HRM – Human resource Planning, Technological change, Restructuring and rightsizing, Empowerment, TQM, Managing ethical issues.	5
02	**Organizational Behavior (OB)** • Introduction to OB Origin, Nature and Scope of Organizational Behavior, Relevance to Organizational Effectiveness and Contemporary issues • Personality: Meaning and Determinants of Personality, Personality development, Personality Types, Assessment of Personality Traits for Increasing Self Awareness • Perception: Attitude and Value, Effect of perception on Individual Decision-making, Attitude and Behavior. • Motivation: Theories of Motivation and their Applications for Behavioral Change (Maslow, Herzberg, McGregor); • Group Behavior and Group Dynamics: Work groups formal and informal groups and stages of group development. Team Effectiveness: High performing teams, Team Roles, cross functional and self-directed team. • Case study	7
03	**Organizational Structure &Design** • Structure, size, technology, Environment of organization; Organizational Roles & conflicts: Concept of roles; role dynamics; role conflicts and stress. • Leadership: Concepts and skills of leadership, Leadership and managerial roles, Leadership styles and contemporary issues in leadership. • Power and Politics: Sources and uses of power; Politics at workplace, Tactics and strategies.	6
04	**Human resource Planning** • Recruitment and Selection process, Job-enrichment, Empowerment - Job-Satisfaction, employee morale. • Performance Appraisal Systems: Traditional & modern methods, Performance Counseling, Career Planning. Training & Development: Identification of Training Needs, Training Methods	5
05	**Emerging Trends in HR** • Organizational development; Business Process Re-engineering (BPR), BPR as a tool for organizational development, managing processes & transformation in HR. Organizational Change, Culture, Environment • Cross Cultural Leadership and Decision Making**:** Cross Cultural Communication and diversity at work**,** causes of diversity, managing. diversity with special reference to handicapped, women and ageing people, intra company cultural difference in employee motivation.	6
06	**HR & MIS** Need, purpose, objective and role of information system in HR, Applications in HRD in various industries (e.g. manufacturing R&D, Public Transport, Hospitals, Hotels and service industries **Strategic HRM** Role of Strategic HRM in the modern business world, Concept of Strategy, Strategic Management Process, Approaches to Strategic Decision Making; Strategic Intent – Corporate Mission, Vision, Objectives and Goals **Labor Laws & Industrial Relations** Evolution of IR, IR issues in organizations, Overview of Labor Laws in India; Industrial Disputes Act, Trade Unions Act, Shops and Establishments Act	10

REFERENCES:

1. Stephen Robbins, Organizational Behavior, 16th Ed, 2013
2. V S P Rao, Human Resource Management, 3rd Ed, 2010, Excel publishing
3. Aswathapa, Human resource management: Text & cases, 6th edition, 2011
4. C. B. Mamoria and S V Gankar, Dynamics of Industrial Relations in India, 15th Ed, 2015, Himalaya Publishing, 15thedition, 2015
5. P. Subba Rao, Essentials of Human Resource management and Industrial relations, 5th Ed, 2013, Himalaya Publishing
6. Laurie Mullins, Management & Organizational Behavior, Latest Ed, 2016, Pearson Publications

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:
Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4. Only Four question need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8015	Professional Ethics and Corporate Social Responsibility (CSR)	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
ILO8015	Professional Ethics and Corporate Social Responsibility (CSR)	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand professional ethics in business
2	To recognize corporate social responsibility

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand rights and duties of business	L1
2	Distinguish different aspects of corporate social responsibility	L2, L4
3	Demonstrate professional ethics	L3
4	Understand legal aspects of corporate social responsibility	L1

Module	Detailed Contents	Hrs
01	**Professional Ethics and Business:** The Nature of Business Ethics; Ethical Issues in Business; Moral Responsibility and Blame; Utilitarianism: Weighing Social Costs and Benefits; Rights and Duties of Business	04
02	**Professional Ethics in the Marketplace:** Perfect Competition; Monopoly Competition; Oligopolistic Competition; Oligopolies and Public Policy **Professional Ethics and the Environment:** Dimensions of Pollution and Resource Depletion; Ethics of Pollution Control; Ethics of Conserving Depletable Resources	08
03	**Professional Ethics of Consumer Protection:** Markets and Consumer Protection; Contract View of Business Firm's Duties to Consumers; Due Care Theory; Advertising Ethics; Consumer Privacy **Professional Ethics of Job Discrimination:** Nature of Job Discrimination. Extent of Discrimination; Reservation of Jobs.	06
04	**Introduction to Corporate Social Responsibility:** Potential Business Benefits—Triple bottom line, Human resources, Risk management, Supplier relations; Criticisms and concerns—Nature of business; Motives; Misdirection. Trajectory of Corporate Social Responsibility in India	05
05	**Corporate Social Responsibility:** Articulation of Gandhian Trusteeship Corporate Social Responsibility and Small and Medium Enterprises (SMEs) in India, Corporate Social Responsibility and Public-Private Partnership (PPP)in India	08
06	**Corporate Social Responsibility in Globalizing India:** Corporate Social Responsibility Voluntary Guidelines, 2009 issued by the Ministry of Corporate Affairs, Government of India, Legal Aspects of Corporate Social Responsibility—Companies Act, 2013.	08

References:

1. Business Ethics: Texts and Cases from the Indian Perspective (2013) by Ananda Das Gupta; Publisher:Springer.
2. Corporate Social Responsibility: Readings and Cases in a Global Context (2007) by Andrew Crane, Dirk Matten, Laura Spence; Publisher:Routledge.
3. Business Ethics: Concepts and Cases, 7th Edition (2011) by Manuel G. Velasquez; Publisher: Pearson, NewDelhi.
4. Corporate Social Responsibility in India (2015) by BidyutChakrabarty, Routledge, NewDelhi.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be a compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:

Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question, paper weightage of each module will be proportional to the number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module3)
4. Only Four questions need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8016	Research Methodology	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
ILO8016	Research Methodology	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand Research and Research Process
2	To acquaint students with identifying problems for research and develop research strategies
3	To familiarize students with the techniques of data collection, analysis of data and interpretation

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Prepare a preliminary research design for projects in their subject matter areas	L3
2	Accurately collect, analyze and report data	L4
3	Present complex data or situations clearly	L3
4	Review and analyze research findings	L1, L4

Module	Detailed Contents	Hrs
01	**Introduction and Basic Research Concepts** Research – Definition; Concept of Construct, Postulate, Proposition, Thesis, Hypothesis, Law, Principle. Research methods vs Methodology Need of Research in Business and Social Sciences, Objectives of Research **Issues** and Problems in Research Characteristics of Research: Systematic, Valid, Verifiable, Empirical and Critical	**09**
02	**Types of Research** Basic Research Applied Research Descriptive Research Analytical Research Empirical Research **2.6** Qualitative and Quantitative Approaches	**07**
03	**Research Design and Sample Design** Research Design – Meaning, Types and Significance Sample Design – Meaning and Significance Essentials of a good sampling Stages in Sample Design Sampling methods/techniques Sampling Errors	**07**
04	**Research Methodology** **4.1** Meaning of Research Methodology **4.2**. Stages in Scientific Research Process: **a.** Identification and Selection of Research Problem **b.** Formulation of Research Problem **c.** Review of Literature **d.** Formulation of Hypothesis **e.** Formulation of research Design **f.** Sample Design **g.** Data Collection **h.** Data Analysis **i.** Hypothesis testing and Interpretation of Data **j.** Preparation of Research Report	**08**
05	**Formulating Research Problem** **5.1** Considerations: Relevance, Interest, Data Availability, Choice of data, Analysis of data, Generalization and Interpretation of analysis	**04**
06	**Outcome of Research** Preparation of the report on conclusion reached. Validity Testing & Ethical Issues Suggestions and Recommendation	**04**

References:

1. Dawson, Catherine, 2002, Practical Research Methods, New Delhi, UBS Publishers Distributors.
2. Kothari, C.R.,1985, Research Methodology-Methods and Techniques, New Delhi, Wiley EasternLimited.
3. Kumar, Ranjit, 2005, Research Methodology-A Step-by-Step Guide for Beginners, (2nd ed), Singapore, Pearson Education

Assessment:

Internal:

Assessment consists of two tests out of which; one should be a compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:

Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question, paper weightage of each module will be proportional to the number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module3)
4. Only Four questions need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8017	IPR and Patenting	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. of 2 Tests					
ILO8017	IPR and Patenting	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand intellectual property rights protection system
2	To promote the knowledge of Intellectual Property Laws of India as well as international treaty procedures
3	To get acquaintance with Patent search and patent filing procedure and applications

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand Intellectual Property assets	L1
2	Support individuals and organizations in capacity building	L5
3	Work for development, promotion, protection, compliance, and enforcement of Intellectual Property and Patenting	L6

Module	Detailed Contents	Hr
01	**Introduction to Intellectual Property Rights (IPR)**: Meaning of IPR, Different category of IPR instruments - Patents, Trademarks, Copyrights, Industrial Designs, Plant variety protection, Geographical indications, Transfer of technology. **Importance of IPR in Modern Global Economic Environment:** Theories of IPR, Philosophical aspects of IPR laws, Need for IPR, IPR as an instrument of development	05
02	**Enforcement of Intellectual Property Rights:** Introduction, Magnitude of problem, Factors that create and sustain counterfeiting/piracy, international agreements, international organizations (e.g. WIPO, WTO) active in IPR enforcement **Indian Scenario of IPR:** Introduction, History of IPR in India, Overview of IP laws in India, Indian IPR, Administrative Machinery, Major international treaties signed by India, Procedure for submitting patent and Enforcement of IPR at national level etc.	07
03	**Emerging Issues in IPR:** Challenges for IP in digital economy, e-commerce, human genome, biodiversity and traditional knowledge etc.	05
04	**Basics of Patents:** Definition of Patents, Conditions of patentability, Patentable and non-patentable inventions, Types of patent applications (e.g. Patent of addition etc), Process Patent and Product Patent, Precautions while patenting, Patent specification Patent claims, Disclosures and non-disclosures, Patent rights and infringement, Method of getting a patent	07
05	**Patent Rules:** Indian patent act, European scenario, US scenario, Australia scenario, Japan scenario, Chinese scenario, Multilateral treaties where India is a member (TRIPS agreement, Paris convention etc.)	08
06	**Procedure for Filing a Patent (National and International):** Legislation and Salient Features, Patent Search, Drafting and Filing Patent Applications, Processing of patent, Patent Litigation, Patent Publication etc, Time frame and cost, Patent Licensing, Patent Infringement **Patent databases:** Important websites, Searching international databases	07

References:

1. Rajkumar S. Adukia, 2007, A Handbook on Laws Relating to Intellectual Property Rights in India, The Institute of Chartered Accountants ofIndia
2. Keayla B K, Patent system and related issues at a glance, Published by National Working Group on PatentLaws
3. T Sengupta, 2011, Intellectual Property Law in India, Kluwer LawInternational
4. Tzen Wong and Graham Dutfield, 2010, Intellectual Property and Human Development: Current Trends and Future Scenario, Cambridge UniversityPress
5. Cornish, William Rodolph & Llewelyn, David. 2010, Intellectual Property: Patents, Copyrights, Trade Marks and Allied Right, 7th Edition, Sweet &Maxwell
6. LousHarns, 2012, The enforcement of Intellactual Property Rights: A Case Book, 3rd Edition, WIPO
7. Prabhuddha Ganguli, 2012, Intellectual Property Rights, 1st Edition,TMH
8. R Radha Krishnan & S Balasubramanian, 2012, Intellectual Property Rights, 1st Edition, Excel Books
9. M Ashok Kumar and mohdIqbal Ali, 2-11, Intellectual Property Rights, 2nd Edition, Serial Publications
10. Kompal Bansal and Praishit Bansal, 2012, Fundamentals of IPR for Engineers, 1st Edition, BS Publications
11. Entrepreneurship Development and IPR Unit, BITS Pilani, 2007, A Manual on Intellectual PropertyRights,
12. Mathew Y Maa, 2009, Fundamentals of Patenting and Licensing for Scientists and Engineers, World Scientific PublishingCompany
13. N S Rathore, S M Mathur, Priti Mathur, Anshul Rathi**,** IPR: Drafting,Interpretation of Patent Specifications and Claims**,** New India PublishingAgency
14. Vivien Irish, 2005, Intellectual Property Rights forEngineers,IET
15. Howard B Rockman, 2004, Intellectual Property Law for Engineers and scientists, Wiley-IEEE Press

Assessment:

Internal:
Assessment consists of two tests out of which; one should be a compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:
Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question, paper weightage of each module will be proportional to the number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module3)
4. Only Four questions need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8018	**Digital Business Management**	**03**	**--**	**--**	**03**	**--**	**--**	**03**

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
ILO8018	**Digital Business Management**	**20**	**20**	**20**	**80**	**--**	**--**	**--**	**100**

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To familiarize with digital business concept
2	To acquaint with E-commerce
3	To give insights into E-business and its strategies

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Identify drivers of digital business	L1, L4
2	Illustrate various approaches and techniques for E-business and management	L3, L4
3	Prepare E-business plan	L3

Module	Detailed content	Hours
1	**Introduction to Digital Business-** Introduction, Background and current status, E-market places, structures, mechanisms, economics and impacts Difference between physical economy and digital economy, **Drivers of digital business**- Big Data & Analytics, Mobile, Cloud Computing, Social media, BYOD, and Internet of Things(digitally intelligent machines/services) Opportunities and Challenges in Digital Business,	09
2	**Overview of E-Commerce** **E-Commerce-** Meaning, Retailing in e-commerce-products and services, consumer behavior, market research and advertisement. B2B-E-commerce-selling and buying in private e-markets, public B2B exchanges and support services, e-supply chains, Collaborative Commerce, Intra business EC and Corporate portals. Other E-C models and applications, innovative EC System-From E- government and learning to C2C, mobile commerce and pervasive computing. EC Strategy and Implementation-EC strategy and global EC, Economics and Justification of EC, Using Affiliate marketing to promote your e- commerce business, Launching a successful online business and EC project, Legal, Ethics and Societal impacts of EC	06
3	**Digital Business Support services**: ERP as e –business backbone, knowledge Tope Apps, Information and referral system **Application Development:** Building Digital business Applications and Infrastructure	06
4	**Managing E-Business**-Managing Knowledge, Management skills for e-business, Managing Risks in e –business Security Threats to e-business -Security Overview, Electronic Commerce Threats, Encryption, Cryptography, Public Key and Private Key Cryptography, Digital Signatures, Digital Certificates, Security Protocols over Public Networks: HTTP, SSL, Firewall as Security Control, Public Key Infrastructure (PKI) for Security, Prominent Cryptographic Applications.	06
5	**E-Business Strategy**-E-business Strategic formulation- Analysis of Company's Internal and external environment, Selection of strategy, E-business strategy into Action, challenges and E-Transition (Process of Digital Transformation)	04
6	**Materializing e-business: From Idea to Realization**-Business plan preparation **Case Studies and presentations**	08

References:

1. A textbook on E-commerce**,** Er Arunrajan Mishra, Dr W K Sarwade,Neha Publishers & Distributors, 2011
2. E-commerce from vision to fulfilment, Elias M. Awad, PHI-Restricted, 2002
3. Digital Business and E-Commerce Management, 6th Ed, Dave Chaffey, Pearson, August 2014
4. Introduction to E-business-Management and Strategy, Colin Combe, ELSVIER, 2006
5. Digital Business Concepts and Strategy, Eloise Coupey, 2nd Edition, Pearson
6. Trend and Challenges in Digital Business Innovation, VinocenzoMorabito, Springer
7. Digital Business Discourse Erika Darics, April 2015, Palgrave Macmillan
8. E-Governance-Challenges and Opportunities in : Proceedings in 2nd International Conference theory and practice of Electronic Governance
9. Perspectives the Digital Enterprise –A framework for Transformation, TCS consulting journal Vol.5
10. Measuring Digital Economy-A new perspective -DOI:10.1787/9789264221796-enOECD Publishing

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test and the other is either a class test or at least 6 assignment on complete syllabus or course project.

End Semester Theory Examination:
Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question paper weightage of each module will be proportional to number of respective lecture hours as mention in the syllabus.**

1. Question paper will comprise of total six question
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4. Only Four question need to be solved.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO8019	Environmental Management	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test1	Test 2	Avg. of 2 Tests					
ILO8019	Environmental Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	Understand and identify environmental issues relevant to India and global concerns
2	Learn concepts of ecology
3	Familiarize environment related legislations

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Understand the concept of environmental management	L1
2	Understand ecosystem and interdependence, food chain etc.	L1
3	Understand and interpret environment related legislations	L1, L5

Module	Detailed Contents	Hrs
01	Introduction and Definition of Environment: Significance of Environment Management for contemporary managers, Career opportunities. Environmental issues relevant to India, Sustainable Development, The Energy scenario.	10
02	Global Environmental concerns: Global Warming, Acid Rain, Ozone Depletion, Hazardous Wastes, Endangered life-species, Loss of Biodiversity, Industrial/Man-made disasters, Atomic/Biomedical hazards, etc.	06
03	Concepts of Ecology: Ecosystems and interdependence between living organisms, habitats, limiting factors, carrying capacity, food chain, etc.	05
04	Scope of Environment Management, Role & functions of Government as a planning and regulating agency. Environment Quality Management and Corporate Environmental Responsibility	10
05	Total Quality Environmental Management, ISO-14000, EMS certification.	05
06	General overview of major legislations like Environment Protection Act, Air (P & CP) Act, Water (P & CP) Act, Wildlife Protection Act, Forest Act, Factories Act, etc.	03

REFERENCES:

1. Environmental Management: Principles and Practice, C J Barrow, Routledge Publishers London, 1999
2. A Handbook of Environmental Management Edited by Jon C. Lovett and David G. Ockwell, Edward Elgar Publishing
3. Environmental Management, **T V Ramachandra and Vijay Kulkarni, TERI Press**
4. Indian Standard Environmental Management Systems — Requirements with Guidance For Use, Bureau Of Indian Standards, February 2005
5. Environmental Management: An Indian Perspective, S N Chary and Vinod Vyasulu, Maclillan India, 2000
6. Introduction to Environmental Management, Mary K Theodore and Louise Theodore, CRC Press
7. Environment and Ecology, Majid Hussain, 3rd Ed. Access Publishing.2015

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test and the other is either a class test or assignment on live problems or course project.

End Semester Theory Examination:
Some guidelines for setting up the question paper. Minimum 80% syllabus should be covered in question papers of end semester examination. **In question paper weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.**

1. Question paper will comprise of total six question.
2. All question carry equal marks
3. Questions will be mixed in nature (for example supposed Q.2 has part (a) from module 3 then part (b) will be from any module other than module 3)
4. Only Four question need to be solved.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL801	Mobile Forensic Lab	--	2	--	--	1	--	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL801	Mobile Forensic Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To make students familiar with the fundamentals of practical mobile forensics.
2	To demonstrate tools and techniques used for data acquisition, analysis and recovery of data from iOS mobile devices.
3	To demonstrate tools and techniques used for data acquisition and recovery of data from Android mobile devices.
4	To demonstrate tools and techniques used for data acquisition from Windows mobile devices.
5	To explore advanced methods for decoding data stored in third-party applications across all smartphones.
6	To explore various scenarios related to real world smartphone forensic investigation.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
Upon Completion of the course the learner/student should be able to:		
1	Explore fundamentals of Practical mobile forensics	L3, L4
2	Demonstrate tools and techniques used for data acquisition, analysis and recovery of data from iOS mobile devices.	L3
3	Demonstrate tools and techniques used for data acquisition and recovery of data from Android mobile devices.	L3
4	Demonstrate tools and techniques used for data acquisition from Windows mobile devices.	L3
5	Explore third-party application data and preference files to support an investigation.	L3, L4
6	Apply the knowledge of forensic investigation to real world scenarios.	L3

Prerequisite: Smartphone Overview, Fundamentals of Analysis, SQLite Introduction, Android Forensics Overview, and Android Backups.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
I	Introduction and Overview of Practical Mobile Forensics	To understand Mobile forensics challenges, Mobile phone Evidence Extraction Process, Practical mobile forensic approaches	**2**	1
II	iOS Device Forensics	To understand Internals of iOS Devices and perform data Acquisition, iOS Data analysis and Recovery, iOS Forensic	**6**	2
III	Android Device Forensic	Setting up Android forensics environment with Android Software Development Kit and applying Pre-Data Extraction Techniques, Android Data Recovery Techniques, Android Forensic Tools	**6**	3
IV	Windows Device Forensics	To demonstrate Windows Phone Data Acquisition	**2**	4
V	Third-Party Application Analysis	To explore Third-Party Applications Artifacts, Messaging Applications and Recovering Attachments	**4**	5
VI	Mini Project	Students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation.	**4**	6

Textbooks:

1. 1.Practical Mobile Forensics, 3rd Edition by Heather Mahalik , Satish Bommisetty, Oleg Skulkin, Rohit Tamma
2. Mobile Forensics – The File Format Handbook , Springer Open Access Book, Christian Hummert,Dirk Pawlaszczyk
3. 3.Learning Android Forensics, Tamma & Tindall

MOOC courses

1. **https://www.udemy.com/course/mobile-computer-forensics/**
2. **https://www.ifsedu.in/cell-phone-forensics/**
3. **https://www.koenig-solutions.com/mobile-forensics-training**
4. **https://www.sans.org/cyber-security-courses/advanced-smartphone-mobile-device forensics/**

List of Experiments/Mini-Project

1. Mobile phone Evidence Extraction Process, Practical mobile forensic approaches.
2. Data Acquisition via custom RAMDisk / JailBreak / iOS Backups.
3. iOS Data analysis and Recovery through timestamps/ SQLite databases/property list.s
4. iOS Forensic with Elcomsoft iOS Forensic Toolkit/Oxygen Forensic Suite/Cellebrite UFED Physical Analyzer/Paraben iRecovery Stick.
5. Android and setting up forensics' environment with Android Software Development Kit and using Pre Data Extraction Techniques.
6. Android Data Extraction Techniques - Manual Data Extraction/ Root Access/ Logical Data Extraction/ Physical Data Extraction.
7. Android Data Recovery by parsing/file carving and using forensics tools such as AFLogical/Autopsy.
8. Windows Phone Data Acquisition using Sideloading, Extracting SMS, Extracting Email, Extracting Application Data.
9. Third-Party Application Artifacts; Messaging Applications and Recovering Attachments; Mobile Browsers; Secure Chat Applications.

Mini Project - Students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

Term Work: Term work shall consist of at least 8 practicals based on the above list and 1 Mini Project. Also, Term work journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An oral exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL802	Dark Web Investigation Lab	--	2	--	--	1	--	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL802	Dark Web Investigation Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To provide hands-on experiences for students to develop critical thinking, research skills, and technical knowledge related to the Dark Web and the Tor network.
2	To understand the structure and functioning of the Dark Web and its implications.
3	To learn about the ethical considerations and legal constraints associated with exploring the Dark Web.
4	To gain familiarity with tools and techniques used for accessing and navigating the Dark Web securely.
5	To explore various aspects of the Dark Web, such as illicit marketplaces, anonymous communication, cryptocurrencies, and cybercriminal activities.
6	To develop skills for conducting Dark Web investigations and gathering intelligence.

Lab Outcomes:

Sr. No.	Lab Outcomes
1	To acquire knowledge about the Dark Web and the Tor network, including their purpose, architecture, and underlying technologies.
2	To understand the ethical implications and legal challenges associated with accessing and exploring the Dark Web.
3	To learn about the tools and techniques used for anonymous browsing and accessing Dark Web websites.
4	To explore various Dark Web marketplaces and understand the types of illegal activities and services available.
5	To analyze the use of cryptocurrencies, such as Bitcoin, on the Dark Web and their role in facilitating anonymous transactions.
6	To develop skills for conducting Dark Web investigations, including gathering intelligence, tracking cybercriminals, and identifying potential threats.

Prerequisite:

1. Familiarity with networking and security fundamentals.
2. Basic knowledge of encryption and anonymity concepts.
3. Virtual machine deployment with pre-installed tools for Dark Web exploration (e.g., Whonix).

Sr. No.	Module	Detailed Content	Hours	LO Mapping
I	Introduction to the Dark Web and the Tor Network	Understanding the surface web, deep web, and Dark Web Overview of the Tor network: Onion routing, Tor hidden services, and Tor relays Legal and ethical considerations for exploring the Dark Web	0	LO3
II	Accessing the Dark Web Securely	Setting up a virtual machine for secure browsing (e.g., Whonix) Configuring Tor browser and understanding its privacy features Proxy chains and VPNs for additional anonymity Best practices for safe and responsible browsing on the Dark Web	1	LO2
III	Exploring Dark Web Marketplaces	Introduction to Dark Web marketplaces: Silk Road, AlphaBay, etc. Understanding the types of products and services available Evaluating the risks and challenges associated with Dark Web marketplaces Case studies of notable investigations and takedowns	1	LO2
IV	Cryptocurrencies on the Dark Web	Overview of cryptocurrencies: Bitcoin, Monero, etc. Role of cryptocurrencies in anonymous transactions on the Dark Web Wallet management and security considerations Tracking and analyzing cryptocurrency transactions for investigative purposes	1	LO4
V	Dark Web Investigations and Intelligence Gathering	Techniques for gathering intelligence from Dark Web sources Open-source intelligence (OSINT) tools for Dark Web investigations Analyzing forums, chat platforms, and social media on the Dark Web Identifying cybercriminal activities and potential threats	1	LO4

Textbooks:

1. The Dark Net: Inside the Digital Underworld by Jamie Bartlett
2. The Dark Web: Breakthroughs in Research and Practice by Information Resources Management Association
3. Dark Web: Exploring and Data Mining the Dark Side of the Web by Hsinchun Chen
4. Understanding the Dark Web by Dimitrios Kavallieros, Dimitrios Myttas, Emmanouil Kermitsis, Euthimios Lissaris, Georgios Giataganas, Eleni Darra

References:

1. Darknet Diaries (Podcast): https://darknetdiaries.com/
2. Hacking the Hacker: Learn From the Experts Who Take Down Hackers by Roger A. Grimes
3. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data by Kevin Mitnick

Resource Tools:

1. Metasploit: Website: https://www.metasploit.com/
2. Wireshark: Website: https://www.wireshark.org/
3. Nmap: Website: https://nmap.org/
4. Burp Suite: Website: https://portswigger.net/burp
5. OWASP ZAP: Website: https://www.zaproxy.org/
6. Hashcat: https://hashcat.net/
7. John the Ripper: https://www.openwall.com/john/
8. Maltego: Website: https://www.maltego.com/

List of Experiments/Mini-Project.

Sr. No.	Detailed Content	LO Mapping
1	Setting up a virtual machine with Whonix for secure browsing on the Dark Web.	LO1
2	Accessing and exploring Tor hidden services, including forums, marketplaces, and chat platforms.	LO1, LO4
3	Analyzing the structure and content of a Dark Web marketplace, identifying products/services, and assessing the credibility of vendors.	LO4
4	Investigating a specific Dark Web marketplace or cybercriminal activity using OSINT tools and techniques.	LO4, LO6
5	Tracking and analyzing cryptocurrency transactions on the Dark Web to identify potential financial trails.	LO5
6	Conducting a threat assessment based on information gathered from Dark Web sources.	LO6, LO3
7	Case study analysis of notable Dark Web investigations and takedowns.	LO6, LO2
8	Ethical discussions on the implications and challenges of Dark Web exploration.	LO1, LO6
9	Select a specific topic or theme on the Dark Web (e.g., drugs, hacking, counterfeit goods) and perform a comprehensive content analysis. Gather data from different Dark Web sources (forums, marketplaces, chat platforms) related to the chosen topic. Analyze the collected data to identify trends, patterns, and key insights regarding the chosen topic. Present findings and implications of the content analysis, including potential risks and societal impact.	LO2, LO6
10	Choose a notable cryptocurrency-related incident or investigation on the Dark Web (e.g., money laundering, illegal transactions). Collect relevant data and blockchain transactions associated with the chosen incident.	LO5
11	Analyze the operational security practices followed by Dark Web marketplaces, forums, or threat actors. Identify common OpSec vulnerabilities and weaknesses observed within the Dark Web ecosystem.	LO4
12.	Example Mini Project suggestion - Exploring Dark Web Drug Markets: Analysis, Trends, and Implications The project focuses on investigating and analyzing the activities within Dark Web drug marketplaces. By collecting and analyzing data from these marketplaces, the project aims to identify trends in drug types, pricing fluctuations, vendor reputation, and customer feedback. The project will utilize data cleaning techniques, statistical analysis, visualization tools, sentiment analysis, and network analysis to extract meaningful insights. The findings of this project will provide a comprehensive understanding of the Dark Web drug trade, offering actionable insights for law enforcement, policymakers, and public health authorities to address the challenges associated with online illicit drug markets.	LO2, LO4, LO3

Mini Project - Students will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSP801	Major Project II	--	12#	--	--	6	--	6

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSP801	Major Project II	--	--	--	--	100	50	150

Course Objectives:

The Project work facilitates the students to develop and prove Technical, Professional and Ethical skills and knowledge gained during graduation program by applying them from problem identification to successful completion of the project by implementing the solution.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Implement solutions for the selected problem by applying technical and professional skills.	L3
2	Analyze impact of solutions in societal and environmental context for sustainable development.	L4
3	Combine best practices along with effective use of modern tools.	L6
4	Develop proficiency in oral and written communication with effective leadership and teamwork.	L6
5	Cultivate professional and ethical behavior.	L6
6	Capture expertise that helps in building lifelong learning experience.	L3

Guidelines:

1. Internal guide has to keep track of the progress of the project and also has to maintain attendance report. This progress report can be used for awarding term work marks.

Project Report Format:

At the end of semester, each group needs to prepare a project report as per the guidelines issued by the University of Mumbai. Report should be submitted in hardcopy. Also, each group should submit softcopy of the report along with project documentation, implementation code, required utilities, software and user Manuals.

A project report should preferably contain at least following details:

- Abstract
- Introduction
- Literature Survey/ Existing system

- Limitation Existing system or research gap
- Problem Statement and Objective
- Proposed System
- Analysis/Framework/ Algorithm
- Design details
- Methodology (your approach to solve the problem) Proposed System
- Experimental Set up

- Details of Database or details about input to systems or selected data
- Performance Evaluation Parameters (for Validation)
- Software and Hardware Set up
- Results and Discussion
- Conclusion and Future Work
- References
- Appendix – List of Publications or certificates

Desirable:
Students should be encouraged -
- to participate in various project competitions.
- to write minimum one technical paper & publish in good journal.
- to participate in national / international conferences.

Term Work:

Distribution of marks for term work shall be done based on following:
- Weekly Log Report
- Completeness of the project and Project Work Contribution
- Project Report (Black Book) (both side print)
- Term End Presentation (Internal)

The final certification and acceptance of TW ensures satisfactory performance in the above aspects.

Oral & Practical:

Oral &Practical examination (Final Project Evaluation) of Project 2 should be conducted by Internal and External examiners approved by University of Mumbai at the end of the semester.

Suggested quality evaluation parameters are as following:
- Relevance to the specialization / industrial trends
- Modern tools used.
- Innovation
- Quality of work and completeness of the project
- Validation of results
- Impact and business value
- Quality of written and oral presentation
- Individual as well as teamwork.