

University of Mumbai



**Syllabus for
B.E. (Cyber Security)
Semester – VII & VIII**

Choice Based Credit System

REV- 2019 'C' Scheme

(With effect from the academic year 2023-24)

University of Mumbai



Syllabus for Approval

Sr. No.	Heading	Particulars
1	Title of Course	B.E. (Cyber Security)
2	Eligibility for Admission	After Passing Third Year Engineering as per the Ordinance 0.6243
3	Passing Marks	40%
4	Ordinances / Regulations (if any)	Ordinances 0.6243
5	No. of years/Semesters:	4 years / 8 semesters
6	Level	Under Graduation
7	Pattern	Semester
8	Status:	New REV-2019 'C' Scheme
9	To be implemented from Academic Year :	With effect from Academic Year: 2023-2024

Offg. Associate Dean
Faculty of Science and Technology

Offg. Dean
Faculty of Science and Technology

Preamble

To meet the challenge of ensuring excellence in engineering education, the issue of quality needs to be addressed, debated and taken forward in a systematic manner. Accreditation is the principal means of quality assurance in higher education. The major emphasis of accreditation process is to measure the outcomes of the program that is being accredited. In line with this Faculty of Science and Technology (in particular Engineering) of University of Mumbai has taken a lead in incorporating philosophy of outcome based education in the process of curriculum development.

Faculty resolved that course objectives and course outcomes are to be clearly defined for each course, so that all faculty members in affiliated institutes understand the depth and approach of course to be taught, which will enhance learner's learning process. Choice based Credit and grading system enables a much-required shift in focus from teacher-centric to learner-centric education since the workload estimated is based on the investment of time in learning and not in teaching. It also focuses on continuous evaluation which will enhance the quality of education. Credit assignment for courses is based on 15 weeks teaching learning process, however content of courses is to be taught in 13 weeks and remaining 2 weeks to be utilized for revision, guest lectures, coverage of content beyond syllabus etc.

There was a concern that the earlier revised curriculum more focused on providing information and knowledge across various domains of the said program, which led to heavily loading of students in terms of direct contact hours. In this regard, faculty of science and technology resolved that to minimize the burden of contact hours, total credits of entire program will be of 170, wherein focus is not only on providing knowledge but also on building skills, attitude and self learning. Therefore in the present curriculum skill based laboratories and mini projects are made mandatory across all disciplines of engineering in second and third year of programs, which will definitely facilitate self learning of students. The overall credits and approach of curriculum proposed in the present revision is in line with AICTE model curriculum.

The present curriculum will be implemented for Second Year of Engineering from the academic year 2021-22. Subsequently this will be carried forward for Third Year and Final Year Engineering in the academic years 2022-23, 2023-24, respectively.

Incorporation and Implementation of Online Contents **from NPTEL/ Swayam Platform**

The curriculum revision is mainly focused on knowledge component, skill based activities and project based activities. Self-learning opportunities are provided to learners. In the revision process this time in particular Revised syllabus of 'C' scheme wherever possible additional resource links of platforms such as NPTEL, Swayam are appropriately provided. In an earlier revision of curriculum in the year 2012 and 2016 in Revised scheme 'A' and 'B' respectively, efforts were made to use online contents more appropriately as additional learning materials to enhance learning of students.

In the current revision based on the recommendation of AICTE model curriculum overall credits are reduced to 171, to provide opportunity of self-learning to learner. Learners are now getting sufficient time for self-learning either through online courses or additional projects for enhancing their knowledge and skill sets.

The Principals/ HoD's/ Faculties of all the institute are required to motivate and encourage learners to use additional online resources available on platforms such as NPTEL/ Swayam. Learners can be advised to take up online courses, on successful completion they are required to submit certification for the same. This will definitely help learners to facilitate their enhanced learning based on their interest.



Preface by Board of Studies Team

It is our honor and a privilege to present the Rev-2019 'C' scheme syllabus of the Bachelor of Engineering in the Cyber Security -- CS (effective from the year 2021-22). AICTE has introduced Cyber Security as one of the nine emerging technology and hence many colleges affiliated with the University of Mumbai has started four years UG program for Cyber Security. As part of the policy decision from the University end, the Board of IT got an opportunity to work on designing the syllabus for this new branch. As the Cyber Security is comparatively a young branch among other emerging engineering disciplines in the University of Mumbai, and hence while designing the syllabus promotion of an interdisciplinary approach has been considered.

The branch also provides multi-faceted scope like better placement and promotion of entrepreneurship culture among students and increased Industry Institute Interactions. Industries' views are considered as stakeholders while the design of the syllabus. As per Industry views only 16 % of graduates are directly employable. One of the reasons is a syllabus that is not in line with the latest emerging technologies. Our team of faculties has tried to include all the latest emerging technologies in the Cyber Security syllabus. Also the first time we are giving skill-based labs and Mini-project to students from the third semester onwards, which will help students to work on the latest Cyber Security technologies. Also the first time we are giving the choice of elective from fifth semester such that students will be mastered in one of the Cyber Security domain. The syllabus is peer-reviewed by experts from reputed industries and as per their suggestions, it covers future emerging trends in Cyber Security technology and research opportunities available due to these trends. .

We would like to thank senior faculties of IT and Computer Department, of all colleges affiliated to University of Mumbai for significant contribution in framing the syllabus. Also on behalf of all faculties we thank all the industry experts for their valuable feedback and suggestions. We sincerely hope that the revised syllabus will help all graduate engineers to face the future challenges in the field of Emerging Areas of Cyber Security.

Program Specific Outcome for graduate Program in Cyber Security

1. Apply Core of Cyber Security knowledge to develop stable and secure Cyber Security Application.
2. Identify the issues of Cyber Security in real time application and in area of cyber security domain.
3. Ability to apply and develop Cyber Security multidisciplinary projects and make it Cyber Security enabled Applications.

Program Structure for Fourth Year Engineering Semester VII & VIII
UNIVERSITY OF MUMBAI
 (With Effect from 2023-24)
Semester VII

Course Code	Course Name	Teaching scheme (Contact Hours)		Credits Assigned					
		Theory	Pract	Theory	Pract	Total			
CSC701	Machine Learning & Cyber Security	3	--	3	--	3			
CSC702	Advance Web X.0 Security	3	--	3		3			
CSDO701X	Department Optional Course – 3	3	--	3	--	3			
CSDO702X	Department Optional Course –4	3	--	3	--	3			
ILO701X	Institute Optional Course – 1	3	--	3	--	3			
CSL701	DevSecOps Lab	--	2	--	1	1			
CSL702	Web Application Security Lab	--	2	--	1	1			
CSL703	ML & Security Lab	--	2	--	1	1			
CSL704	Open-Source Intelligence (OSINT) Lab	--	2	--	1	1			
CSP701	Major Project I	--	6#	--	3	3			
Total		15	14	15	7	22			
Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test1	Test2	Avg					
CSC701	Machine Learning & Cyber Security	20	20	20	80	3	--	--	100
CSC702	Advance Web X.0 Security	20	20	20	80	3	--	--	100
CSDO701X	Department Optional Course – 3	20	20	20	80	3	--	--	100
CSDO702X	Department Optional Course –4	20	20	20	80	3	--	--	100
ILO701X	Institute Optional Course – 1	20	20	20	80	3	--	--	100
CSL701	DevSecOps Lab	--	--	--	--	--	25	25	50
CSL702	Web Application Security Lab	--	--	--	--	--	25	25	50
CSL703	ML & Security Lab	--	--	--	--	--	25	25	50
CSL704	Open-Source Intelligence (OSINT) Lab	--	--	--	--	--	25	25	50
CSP701	Major Project I	--	--	--	--	--	25	25	50
Total		--	--	100	400	--	125	125	750

indicates work load of Learner (Not Faculty), for Major Project

CSDO701X	Department Optional Course –3
CSDO7011	Advance Cloud Computing Security
CSDO7012	Software Testing & Quality Assurance (STQA)
CSDO7013	Storage Area Network
CSDO7014	Supervisory Control and Data acquisition (SCADA) Security

CSDO702X	Department Optional Course –4
CSDO7021	Cyber Security Management
CSDO7022	User Interface Design with Security
CSDO7023	MANET
CSDO7024	Information retrieval system

Institute Level Optional Course (ILO)

Every student is required to take one Institute Elective Course for Semester VII, which is not closely allied to their disciplines. Different sets of courses will run in the both the semesters.

ILO701X	Institute Optional Course – 1 (Common for all branches will be notified)
ILO7011	Product Lifecycle Management
ILO7012	Reliability Engineering
ILO7013	Management Information System
ILO7014	Design of Experiments
ILO7015	Operation Research
ILO7016	Cyber Security and Laws
ILO7017	Disaster Management and Mitigation Measures
ILO7018	Energy Audit and Management
ILO7019	Development Engineering

Program Structure for Fourth Year Engineering Semester VII & VIII
UNIVERSITY OF MUMBAI
(With Effect from 2023-24)

Semester VIII

Course Code	Course Name	Teaching Scheme (Contact Hours)				Credits Assigned			
		Theory		Pract		Theory	Pract	Total	
CSC801	Malware Analysis	3		--		3	--	3	
CSDO801X	Department Optional Course – 5	3		--		3	--	3	
CSDO802X	Department Optional Course – 6	3		--		3	--	3	
ILO801X	Institute Optional Course – 2	3		--		3	--	3	
CSL801	Mobile Forensic Lab	--		2		--	1	1	
CSL802	Dark Web Investigation Lab	--		2		--	1	1	
CSP801	Major Project II	--		12#		--	6	6	
Total		12		16		12	8	20	
Course Code	Course Name	Examination Scheme							
		Theory					Term Work	Pract	Total
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
CSC801	Malware Analysis	20	20	20	80	3	--	--	100
CSDO801X	Department Optional Course – 5	20	20	20	80	3	--	--	100
CSDO802X	Department Optional Course – 6	20	20	20	80	3	--	--	100
ILO801X	Institute Optional Course – 2	20	20	20	80	3	--	--	100
CSL801	Mobile Forensic Lab	--	--	--	--	--	25	25	50
CSL802	Dark Web Investigation Lab	--	--	--	--	--	25	25	50
CSP801	Major Project II	--	--	--	--	--	100	50	150
Total		--	--	80	320	--	150	100	650

indicates workload of Learner (Not Faculty), for Major Project



Students group and load of faculty per week.

Mini Project 1 and 2:

Students can form groups with minimum 2 (Two) and not more than 4 (Four)

Faculty Load: 1 hour per week per four groups.

Major Project 1 and 2:

Students can form groups with minimum 2 (Two) and not more than 4 (Four)

Faculty Load: In Semester VII – ½ hour per week per project group.

In Semester VIII – 1 hour per week per project group

CSDO801X	Department Optional Course – 5
CSDO8011	Social & Ethical issues of the Internet
CSDO8012	IoTs & Embedded Security
CSDO8013	Cognitive Psychology in Cyber Security
CSDO8014	Intelligent Forensic

CSDO802X	Department Optional Course –6
CSDO8021	Advance Blockchain Technology
CSDO8022	Metaverse
CSDO8023	Green IT
CSDO8024	Cyber Security laws & legal aspects

IOTIO801X	Institute Optional Course – 2 (Common for all branches will be notified)
ILO8011	Project Management
ILO8012	Finance Management
ILO8013	Entrepreneurship Development and Management
ILO8014	Human Resource Management
ILO8015	Professional Ethics and CSR
ILO8016	Research Methodology
ILO8017	IPR and Patenting
ILO8018	Digital Business Management
ILO8019	Environmental Management

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSC701	Machine Learning & 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					
CSC701	Machine Learning & Cyber Security	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand basic concepts of artificial intelligence.
2	To develop problem solving ability using machine learning algorithms.
3	To examine clustering and classification based on machine learning techniques.
4	To study anomaly detection and analyze network traffic.
5	To detect, classify and analyze malware.
6	To understand Cyber Security Mechanisms Using Deep Learning techniques.

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 role of artificial intelligence in cyber security.	L1, L2
2	Use machine learning algorithms for solving the security issues.	L1, L2, L3
3	Provide solutions for real time security problems using machine learning algorithms.	L1, L2, L3
4	Develop awareness of latest trends and advances in security using machine learning.	L1, L2, L3, L4, L5, L6
5	Detect, classify and analyze malware.	L1, L2, L3, L4
6	Analyze Cyber Security Mechanisms Using Deep Learning techniques.	L1, L2, L3, L4

Prerequisite: Linear algebra, Probability theory and Basic statistics

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Linear algebra Basic Probability and Distributions-Binomial, Poisson, Normal, Exponential, Gaussian Basic statistics Eigen vectors and Eigenvalues	02	-
I	Introduction to Artificial Intelligence (AI)	What is AI, its goals, types of AI Types of agents, intelligent agent, agent environment search algorithms	04	CO1
II	Basics of Machine Learning in Cyber security	Definitions of machine Introduction to Machine Learning: Supervised Machine Learning, Unsupervised Machine Learning, Semi-supervised Machine Learning, Reinforcement Machine Learning Regression and its types. Applications of machine learning Real-World Uses of Machine Learning in cyber security, Spam Fighting: An Iterative Approach Limitations of Machine Learning in Security	06	CO2
	Self-learning topics	Case Studies on Taxonomy of machine learning algorithms		
III	Clustering and Classification	Supervised Classification Algorithms: Naive Bayes Classifier, Support Vector Machines (SVM), Decision Trees, Decision Forest, Nearest Neighbor, Neural Network. Practical Considerations in Classification: Selecting a Model Family, Training Data Construction, Feature Selection, Overfitting and Underfitting, Choosing Thresholds and Comparing Models. Clustering: K-means, Hierarchical clustering, Fuzzy C-Means Clustering, Density-Based Clustering, State of the Art of Clustering Applications. Optimization techniques	08	CO3
	Self-learning topics	Exploiting XSS Vulnerability in C&C Panels to Detect Malwares		
IV	Anomaly detection and Network Traffic Analysis Using ML	Anomaly Detection: Feature Engineering for Anomaly Detection Anomaly Detection with Data and Algorithms Challenges of Using Machine Learning in Anomaly Detection Network Traffic Analysis: Theory of Network Defense Building a Predictive Model to Classify Network Attacks.	6	CO4
	Self-learning topics	Network Anomaly Detection Using k-means Stages of a network attack		
V	Malware: detection & analysis	Malware Detection using support vector machine. Maximizing the Margin and Hyperplane Optimization, Lagrange Multiplier, Kernel Methods Permission-Based Static Android Malware Detection Using SVM. Malware Analysis: Defining Malware Classification, Malware: Behind the Scenes, Feature Generation, Data Collection, Feature Selection, From Features to Classification, How to Get Malware Samples and Labels	8	CO5

	Self-learning topics	API Call-Based Static Android Malware Detection		
VI	Deep Learning in Security	Introduction to deep learning in cyber security Cyber Security Mechanisms Using Deep Learning Algorithms Applying deep learning in various use cases	05	CO6
	Self-learning topics	Network Cyber threat Detection		

Textbooks:

1. Machine Learning and Security by Clarence Chio, David Freeman, O'Reilly Media; 1st edition, 2018
2. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
3. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s): Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

References:

1. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.
2. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.
3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.
4. Tom Mitchell. Machine Learning. McGraw Hill, 1997.

Online References:

1. [What Is Machine Learning in Security? - Cisco](#)
2. [5 Top Machine Learning Use Cases for Security](#)

MOOC Courses:

1. [NOC: Introduction to Machine Learning\(Course sponsored by Aricent\), IIT Madras](#)
2. <https://nptel.ac.in/courses/106/106/106106202/>
3. [Free Online Course: Machine Learning Security from Amazon | Class Central](#)

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	Practical/Oral	Tutorial	Total
CSC702	Advance Web X.0 Security	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					
CSC702	Advance Web X.0 Security	20	20	20	80	--	--	--	100

Sr. No.	Course Objectives:
The course aims:	
1	To familiarize yourself with advanced web application security fundamentals.
2	To understand the methodical way of discovering vulnerabilities and plan strategies for mitigation.
3	To gain insight about the web application Penetration testing methods
4	To understand authentication and session management in web applications.
5	To discover and defend client-side web security attacks.
6	To gain insight about injection attacks on web datastore and web server.

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	To identify and describe web application security threats.	L1, L2
2	To review, discover and manage vulnerabilities of web Applications and plan strategies for mitigation.	L1, L2, L3, L4
3	To understand the web penetration testing workflow and organize a checklist for penetration testing with the help of usage of tools.	L1, L2, L3, L4
4	To apply access control, authorization and authentication mechanisms in web applications.	L1, L2, L3
5	To explore various client -side web application security aspects.	L1, L2, L3
6	To explain various injection attacks on data and server in web application	L1, L2, L3

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Introduction to Web applications Cookies, Session, Headers, Same-origin , Terminology And Tools	02	-
I	Introduction to Web X.0 security	N/W security vs application security, open web application security projects (OWASP), OWASP Top 10 flaws, Security fundamentals: Input validation, Attack surface reduction, classifying and prioritizing threats	04	CO1
II	Vulnerability Assessment	Defensive Software Architecture - Analyzing Feature Requirements, Authentication and Authorization Comprehensive Code Reviews: How to start code review, Archetypical vulnerabilities Versus Custom Logic Bugs, Secure coding Anti-patterns. Vulnerability Discovery- Security Automation (Static, Dynamic analysis), Vulnerability Regression Testing, Responsible Disclosure Programs Vulnerability Analysis- Vulnerability Management: Reproducing Vulnerabilities, Ranking Vulnerability Severity, Common and Advanced Vulnerability Scoring System Regression Testing, Mitigation Strategies	07	CO2
III	Web application Penetration testing	Web Intrusion/penetration Test workflow: OWASP checklist for web intrusion tests, Burp Pro based. Identifying hidden web contents Personal information, Email addresses, Credentials, CMS, files, Administration URL Common web page testing checklist entry points, backend or third-party web services, API calls, check flaws, errors, authentication at various levels and privileges, header security best practices, cookie/sessionID, duration, client source code, logout exits. Special page testing checklist Login page, CAPTCHA, Registration page, reset password, Upload Page Reporting	07	CO3
IV	Web Authentication, Session management	Access Control Overview: Basic components of access control, High-level access control process. Authentication fundamentals; Two-factor and three-factor authentication; Web Application Authentication, securing password-based authentication, securing web authentication mechanism. Authorization Fundamentals, Goals, Detailed authorization check process, Types of permissions, Authorization layers, Controls by layers, Custom authorization mechanisms, client-side attacks, Time of Check to Time of Use (TOCTTOU) Exploit, Web Authorization Best Practices, Attacks against authorization, Session Management Fundamentals, why do we need session management, Weaknesses in Token Generation, Weaknesses in Session Token Handling, Attacks against sessions, Securing web application session management, Session Management Best Practices	07	CO4

V	Client-side Security	Cross-site scripting (XSS): XSS Discovery and Exploitation, Stored XSS, Reflected XSS, DOM-Based XSS, Mutation-Based XSS Defending Against XSS Attacks: Anti-XSS Coding Best Practices, Sanitizing User Input, Content Security Policy for XSS Prevention Cross-Site Request Forgery (CSRF): Query Parameter Tampering, Alternate GET Payloads, CSRF Against POST Endpoints Defending Against CSRF Attacks: Header Verification, CSRF Tokens, Anti-CSRF Coding Best Practices	06	CO5
VI	Datastore and Server Security	SQL Injection; Setting Database Permissions; Stored Procedure Security; Insecure Direct Object References; Injecting into NoSQL, injecting into XPath, Injecting OS Commands, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, Injecting into Mail Services	06	CO6

Text Books:

1. Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman O'Reilly (Module 2)
2. Web application Security a beginners guide by Bryan Sullivan and Vincent Liu TMH
3. The Web Application Hacker's handbook, Defydd Stuttard, Wiley Publishing
4. Practical Web Penetration Testing by Gus khawaja, packt publication

References:

1. Joel Scambray, Vincent Liu , Caleb Sima ,“Hacking exposed”, McGraw - Hill
2. Professional Pen Testing for Web application, Andres andreu, wrox press
3. Web Application Vulnerabilities: Detect, Exploit, Prevent,by Steven Palmer,Syngress publishing

Online References: 1. <https://www.udemy.com/course/web-application-security/>

2. <https://owasp.org/>

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
CSDO7011	Advanced Cloud Computing 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					
CSDO7011	Advanced Cloud Computing Security	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To understand the concept of security and its significance in the context of cloud computing.
2	To study cloud infrastructure security and mitigation techniques
3	To understand the working of Data center and Data Protection techniques
4	To develop a comprehensive understanding of challenges and solutions in secure identity management for cloud environments
5	To study Compliance and Security Audits policies for cloud data
6	To understand the Cloud Native Security

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 security and its importance in the context of cloud computing.	L2
2	Analyze cloud infrastructure security and apply different mitigation techniques.	L3, L4
3	Apply different data protection techniques in data centers.	L3
4	Design and implement secure identity management solutions for cloud environments	L6
5	Interpret and appropriately apply the policies on Compliance and Security Audits for cloud data	L2, L3
6	Demonstrate cloud security tools for designing, implementing, and managing cloud-native security	L2, L6

Prerequisite: Knowledge of Cloud Computing and Cryptography and Network Security

DETAILED SYLLABUS

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basics of cloud computing, network and system security	2	

I	Fundamentals Of Cloud Security Concepts	What is security, why is it required in cloud computing, Different types of security in cloud, attacks, and vulnerabilities Cloud Security Concepts - CIA Triad (Confidentiality, integrity, availability), privacy, authentication, non-repudiation, access control, defence in depth, least privilege, Traditional vs Cloud Security, importance, challenges in different cloud environment (public, private, hybrid, multi-cloud) Self-Learning Topic: Real-world Example of CIA Triad - Bank ATM	5	CO1
II	Cloud Infrastructure Security: Threats and Mitigation Techniques	Secure Infrastructure architecture Infrastructure Security: Network Level, Host Level and Application Level Common attack vectors and threats Mitigation techniques- Isolation, Virtualization and Segmentation, Intruder Detection and prevention, Firewall, OS Hardening and minimization, Verified and measured boot. Self-Learning Topics: DoS, Man-in-the-Cloud, Insecure APIs, Insider Threats, Cookie Poisoning, Cloud Malware Injection,	7	CO2
III	Cloud Data Security	Cloud security principles Aspects of Data Security Mitigation techniques: Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key Data center Security and Data Protection: Physical and network data center security, Implementation of security in Virtual Data centers, East-west Traffic Protections, Types of firewall, IDS and IPS, DMZ Provider Data and Its Security Self-Learning Topics: Case studies: Capital One Data Breach, Uber's AWS Data Breach, Dow Jones Data Leak, Accenture AWS S3 Data Exposure, Verizon AWS S3 Data Exposure	6	CO3
IV	Secure Identity Management in The Cloud: Challenges And Solutions	IAM overview, Trust Boundaries and IAM, Architecture / Lifecycle process, IAM standards and protocols, IAM Challenges Cloud Authorization Management: Identity management - User Identification, Authentication and Authorization Roles-based Access Control - Multi-factor authentication, Single Sign-on, Identity Federation Cloud Service Provider IAM Practice Self-Learning Topic: IAM service in AWS	6	CO4
V	Disaster Recovery Auditing: Mitigating Risk and Ensuring Compliance	Cloud disaster recovery, types of disasters recovery, benefits of disaster recovery, cloud disaster recovery planning Privacy: Data life cycle, key privacy concerns in cloud, privacy risk management and compliance, legal and regulatory implications, Cloud Audit and Compliance: Internal Policy Compliance, Governance, Risk, and Compliance (GRC), Benefits, GRC Program Implementation, Cloud Security Alliance, Self-Learning Topics: HIPAA, ISO, PCI	7	CO5
VI	Cloud Native Security in The Modern Organization	Overview of Cloud Native Security, where it fits in the Modern Organization, purpose of Security, Cloud Native Security Architecture, Threats to Cloud Native Applications 3 R's and 4 C's of Cloud Native Security Cloud Native Security Controls, Cloud Native Security Tools, Cloud Native security architecture principles, DevSecOps,	6	CO6

		How to Measure the Impact of Security, Cloud-Native Application Protection Platform (CNAPP) Self Learning Topic: Case study on Secure the Cloud		
--	--	---	--	--

Textbooks:

1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather, Subra Kumaraswamy, and Shahed Latif, O'Reilly
2. Cloud Native Security Cookbook: Recipes for a Secure Cloud 1st Edition by Josh Armitage, O'Reilly
3. Cloud Security: A Comprehensive Guide to Secure Cloud Computing by Ronald L. Krutz and Russell Dean Vines, Wiley

References:

1. "Securing the Cloud: Cloud Computer Security Techniques and Tactics" by Vic (J.R.) Winkler, SYNGRESS
2. "Identity and Access Management as a Service: Security as a Service" by Wei Meng Lee
3. Cloud Security for Dummies by Ted Coombs, O'Reilly

Online References:

1. <https://www.coursera.org/learn/cloud-computing-security#about>
2. <https://www.coursera.org/specializations/cybersecurity-cloud>
3. <https://www.edx.org/course/cloud-computing-security>
4. <https://www.ibm.com/topics/cloud-security>
5. <https://www.vmware.com/topics/glossary/content/east-west-security.html>
6. <https://www.vmware.com/topics/glossary/content/data-center-security.html>
7. <https://cloud.google.com/learn/what-is-disaster-recovery>
8. https://www.splunk.com/en_us/blog/learn/cloud-native-security.html

1. 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	Pract/Oral	Tutorial	Total
CSDO7012	Software Testing & Quality Assurance (STQA)	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					
CSDO7012	Software Testing & Quality Assurance (STOA)	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To provide students with knowledge in Software Testing techniques.
2	To provide knowledge of Black Box and White Box testing techniques.
3	To provide skills to design test case plans for testing software.
4	To prepare test plans and schedules for testing projects.
5	To understand how testing methods can be used in a specialized environment.
6	To understand how testing methods can be used as an effective tool in providing quality assurance concerning software.

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	Investigate the reason for bugs and analyze the principles in software testing to prevent and remove bugs.	L1, L2, L3, L4
2	Understand various software testing methods and strategies.	L1, L2
3	Manage the testing process and testing metrics.	L1, L2, L3, L4
4	Understand fundamental concepts of software automation and use automation tools.	L1, L2
5	Apply the software testing techniques in the real time environment.	L1, L2, L3
6	Use practical knowledge of a variety of ways to test software and quality attributes.	L1, L2, L3

Prerequisite: Programming Language (C++, Java), Software Engineering



DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Software Engineering Concepts, Basics of programming Language	02	
I	Testing Methodology	Introduction, Goals of Software Testing, Software Testing Definitions, Model for Software Testing, Effective Software Testing vs Exhaustive Software Testing, Software Failure Case Studies, Software Testing Terminology, Software Testing Life Cycle (STLC), Software Testing methodology, Verification and Validation, Verification requirements, Verification of high-level design, Verification of low-level design, validation. Self-learning Topics: Study any system/application, find requirement specifications and design the system. Select software testing methodology suitable to the application.	07	CO1
II	Testing Techniques	Dynamic Testing: Black Box Testing: Boundary Value Analysis, Equivalence Class Testing, State Table Based testing, Cause-Effect Graphing Based Testing, Error Guessing. White Box Testing Techniques: need, Logic Coverage Criteria, Basis Path Testing, Graph Matrices, Loop Testing, Data Flow testing, Mutation testing. Static Testing. Validation Activities: Unit validation, Integration, Function, System, Acceptance Testing. Regression Testing: Progressive vs. Regressive, Regression Testing, Regression Testability, Objectives of Regression Testing, Regression Testing Types, Define Problem, Regression Testing Techniques. Self-learning Topics: Select the test cases (positive and negative scenarios) for the selected system and Design Test cases for the system using any two studied testing techniques.	09	CO2
III	Managing the Test Process	Test Management: test organization, structure and of testing group, test planning, detailed test design and test Specification. Software Metrics: need, definition and Classification of software matrices. Testing Metrics for Monitoring and Controlling the Testing Process: attributes and corresponding metrics, estimation model for testing effort, architectural design, information flow matrix used for testing, function point and test point analysis. Efficient Test Suite Management: minimizing the test suite and its benefits, test suite minimization problem, test suite prioritization of its type, techniques and measuring effectiveness. Self-learning Topics: Design quality matrix for your selected system	08	CO3
IV	Test Automation	Automation and Testing Tools: need, categorization, selection and cost in testing tool, guidelines for testing tools. Study of testing tools: JIRA, Bugzilla, TestDirector and IBM Rational Functional Tester, Selenium etc. Self-learning Topics: Write down test cases, execute and manage using studied tools	05	CO4

V	Testing for specialized environment	Agile Testing, Agile Testing Life Cycle, Testing in Scrum phases, Challenges in Agile Testing Testing Web based Systems: Web based system, web technology evaluation, traditional software and web-based software, challenges in testing for web-based software, testing web-based testing. Self-learning Topics: Study the recent technical papers on software testing for upcoming technologies (Mobile, Cloud, Blockchain, IoT)	04	CO5
VI	Quality Management	Software Quality Management, McCall's quality factors and Criteria, ISO 9000:2000, SIX sigma, Software quality management Self-learning Topics: Case Studies to Identify Quality Attributed Relationships for different types of Applications (Web based, Mobile based etc.)	04	CO6

Textbooks:

1. Software Testing Principles and Practices Naresh Chauhan Oxford Higher Education
2. Software Testing and quality assurance theory and practice by Kshirasagar Naik, Priyadarshi Tripathy, Wiley Publication

References Books:

1. Effective Methods for Software Testing, third edition by Willam E. Perry, Wiley Publication
2. Software Testing Concepts and Tools by Nageswara Rao Pustular , Dreamtech press

Online References:

1. www.swayam.gov.in
2. www.coursera.org
3. [http://onlinelibrary.wiley.com/journal/10.1002/\(ISSN\)1099-1689](http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1099-1689)
4. https://onlinecourses.nptel.ac.in/noc17_cs32/preview
5. https://www.youtube.com/channel/UC8w8_H_1uDfi2ftQx7a64uQ

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	Practical	Tutorial	Total
CSDO7013	Storage Area Network	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					
CSDO7013	Storage Area Network	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	To provide the knowledge of types of Storage Network.
2	To examine NAS technology and its applications in Storage Area Networks.
3	To study Emerging Technologies in SAN.
4	To define backup, recovery, disaster recovery and business continuity in the storage area Network.
5	To learn cloud-based storage virtualization technologies in SAN.
6	To understand the logical and physical components of storage infrastructures.

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 the limitations of the client-server architecture and evaluate the need for data protection and storage centric architectures such as Intelligent storage system.	L1, L2
2	Understand various SAN technologies.	L1, L2
3	Analyze and examine NAS technologies and its application in Storage Area Network.	L1, L2, L4
4	Explain Different I/O Techniques in SAN.	L1, L2
5	Elaborate Cloud based storage virtualization technologies in SAN.	L1, L2, L4
6	Explain and build Storage infrastructure management with security.	L1, L2, L3

Prerequisite: Operating System, Computer Organization, Computer Network

DETAILED SYLLABUS:



Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Components of a Storage System Environment, Disk drive components, RAID levels, Cloud Computing	02	--
I	Introduction to Storage Area Network	Intelligent Storage Systems (ISS) , Storage Provisioning, Types of Intelligent Storage Systems Evolution of Storage System: Server-Centric IT Architecture and its Limitations, Storage-Centric IT Architecture and its Advantages, SAN & its advantages. Self-learning Topics: Case Study on Replacing a server with Storage networks.	04	CO1
II	Networked Attached Storage & its application	Local File Systems: File systems and databases, Journaling, Snapshots, Volume manager Network File Systems, and File Servers: Network Attached Storage (NAS), Performance bottlenecks in file servers, Acceleration of network file systems, Case study: The Direct Access File System (DAFS), Shared Disk File Systems: A case study The General Parallel File System (GPFS), Applying NAS solution: NAS workload characterization, applying NAS to departmental workloads, enterprise web workloads, and specialized workloads; Considerations when integrating SN and NAS: Differences and similarities, the need to integrate, future storage connectivity and integration. Self-learning Topics: Case study on Successful SAN Deployment steps.	07	CO2
III	Storage I/O Techniques	The Physical I/O Path from the CPU to the Storage System, SCSI, The Fiber Channel Protocol Stack, Fiber Channel SAN, IP Storage, InfiniBand-based Storage Networks, Fiber Channel over Ethernet (FCoE). Self-learning Topics: Case Study on FCoE SAN.	06	CO3
IV	Backup and Data Archive	Introduction to Business Continuity: Information Availability, BC Terminology, BC Planning Lifecycle, Failure Analysis, Business Impact Analysis Backup and Archive: Backup Purpose, Backup Considerations, Backup Granularity, Recovery Considerations, Backup Methods, Backup Architecture, Backup and Restore Operations, Backup Topologies Self-learning Topics: Case Study on Replication strategy	06	CO4
V	Storage Area Network as a Service for Cloud Computing & Virtualization	Virtualization and the cloud: Cloud infrastructure virtualization, Cloud platforms, Storage virtualization, SAN virtualization Virtualization Appliances: Black Box Virtualization, In-Band Virtualization Appliances, Out-of-Band Virtualization Appliances High Availability for Virtualization Appliances, Appliances for Mass Consumption. Storage Automation and Virtualization: Policy-Based Storage Management, Application-Aware Storage Virtualization, Virtualization-Aware Applications. Self-learning Topics: Case study on symmetric and asymmetric virtualization in networks.	06	CO5



VI	Securing and Managing storage infrastructure	Securing and Storage Infrastructure: Information Security Framework, Risk Triad, Storage Security Domains, Security Implementations in Storage Networking, Securing Storage Infrastructure in Virtualized and Cloud Environments. Managing storage infrastructure: Monitoring the Storage Infrastructure, Storage Infrastructure Management activities, Storage Infrastructure Management, Challenges, Information Lifecycle Management, Storage Tiering. Self-learning Topics: Case study on SAN Management and Standards.	08	CO6
----	--	--	----	-----

Textbooks:

1. G. Somasundaram, Alok Shrivastava, EMC Educational Services, "Information Storage and Management", Wiley India.
2. Storage Virtualization, Author: Clark Tom, Publisher: Addison Wesley Publishing Company
3. Ulf Troppens, Wolfgang Muller-Friedt, Rainer Wolafka, "Storage Networks Explained" Wiley Publication
4. "Introduction to Storage Area Networks" Jon Tate, Pall Beck, Hector Hugo Ibarra, Shanmuganathan Kumaravel, Libor Miklas, IBM Redbooks.

References:

1. Richard Barker and Paul Massiglia, iStorage Area Network Essentials: A Complete Guide to Understanding and Implementing SANs, Wiley India.
2. Storage Networks: The Complete Reference, by Robert Spalding (Author)
3. "Storage Network Management and Retrieval", Vaishali Khairnar, Nilima Dongre. Wiley

Online References:

1. /dhttps://www.itprc.com/ultimate-guide-to-storage-area-networks/
2. https://www.techtarget.com/searchstorageefinition/storage-area-network-SAN
3. https://www.snia.org/educational-library/object-storage-trends-use-cases-2021
4. https://www.sciencedirect.com/topics/computer-science/network-attached-storage
5. https://www.techtarget.com/searchstorage/tip/Understand-your-storage-infrastructure-management
6. https://sites.google.com/site/testwikiforfirstciscolab/shd/14-securing-the-storage-infrastructure
7. https://www.techtarget.com/searchdatabackup/tip/What-is-the-difference-between-archives-and-backups.

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	Practical	Tutorial	Total
CSDO7014	Supervisory Control and Data acquisition (SCADA) 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					
CSDO7014	Supervisory Control and Data acquisition (SCADA) Security	20	20	20	80	--	--	--	100

Course Objectives:

The course aims:

Sr. No.	Course Objectives
1	To understand SCADA systems operations and measuring the effectiveness of viable security controls.
2	To identify the challenges in securing current SCADA systems.
3	To interpret incident response, prioritization and notification in SCADA systems.
4	To plan SCADA contingency processes for Disaster Recovery and Business Continuity.
5	To assimilate Project Management for SCADA Systems.
6	Study new age SCADA systems utilities.

Course Outcomes:

On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
1	Understand SCADA systems operations and measuring the effectiveness of viable security controls.	L1, L2
2	Identify and analyze the challenges in securing current SCADA systems.	L1, L2, L4
3	Interpret incident response, prioritization, and notification in SCADA systems.	L1, L2, L3
4	Plan SCADA contingency processes for Disaster Recovery and Business Continuity.	L1, L2, L3
5	Assimilate Project Management for SCADA Systems.	L1, L2, L3
6	Demonstrate new age SCADA systems utilities.	L1, L2

Prerequisite: Computer Network and Security

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Computer Network and Security	02	
I	Industrial Control Systems and Metrics Framework	Evolution of Industrial Control Systems, ICS Industrial Sectors and their Interdependencies, ICS Operation and Components, ICS versus IT Systems Security, Metrics: Security group knowledge, Attack group knowledge, Access, Vulnerabilities, Damage potential, Detection and Recovery, Defining cybersecurity metrics. Self-Study: Other Types of Control Systems	05	CO1
II	The Cyberthreat to SCADA systems and Commercial product vulnerabilities	Directed attacks, Thwarted attacks, Successful attacks, Identified incidents, Microsoft: the leading supplier of software with vulnerabilities, Other major vendors: Oracle, IBM Google, Adobe, Apple, and Cisco. Self-Study: Improvement of SCADA Security	07	CO2
III	Incident Response and SCADA	Difficulties with SCADA and incident response, Incident analysis, Incident prioritization, Incident notification, choosing a containment strategy, Evidence gathering and handling, Basic forensics for standard computers, Identifying the attacker, Eradication and recovery, Evidence retention. Self-Study: Case study: DHS (Department of Homeland Security)	07	CO3
IV	Disaster recovery and business continuity of SCADA	Business continuity process, Types of plans, Examples of SCADA systems at risk, SCADA contingency planning process, SCADA system contingency plan development, Recovery phase, Sequence of recovery activities, Recovery procedures, Recovery escalation and notification, Reconstitution phase, Plan appendices, Maintenance of data security, integrity, and backup, Protection of resources, Identification of alternate storage and processing facilities. Self-Study: Client/server systems and Telecommunications systems	07	CO4
V	Project management for SCADA systems	Introduction, Areas of knowledge needed, Similarities and differences with the SCADA community, managing stakeholders and projects, how to be successful with SCADA implementations. Self-Study: Case study: SCADA implementations	05	CO5
VI	Supervisory control applications & Operator interface	Operating System Utilities, SCADA System Utilities, Program Development Tools, Access-Control Mechanisms, Standard System Displays, Logs and Reports. Self-Study: Standardized APIs, Site/Industry-Specific Displays, Historical Trending	06	CO6

Textbooks:

1. Guide to Industrial Control Systems (ICS) Security, Revision 2 by Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn
2. Handbook of SCADA/Control Systems, Second Edition by Robert Radvanovsky, Jacob Brodsky
3. Cybersecurity for SCADA Systems, Second Edition by William Shaw
4. Cyber-security of SCADA and Other Industrial Control Systems By Edward J. M. Colbert, Alexander Kott

References Books:

1. "Industrial Automation and Control System Security Principles" by Ronald L. Krutz and Russell Dean Vines
2. "SCADA Security: What's Broken and How to Fix It" by Robert Radvanovsky and Jacob Brodsky
3. "SCADA Security: Protecting Critical Infrastructure Systems" by Jack Whitsitt
4. "SCADA and Me: A Book for Children and Management" by Robert M. Lee

Online References:

1. <https://www.inductiveautomation.com/resources/article/what-is-scada>
2. <https://www.dpstele.com/scada/introduction-fundamentals-implementation.php>
3. <https://www.parasyn.com.au/scada-services-rtu-solutions/#whataretheapplicationsusedinscada?>
4. <https://www.parasyn.com.au/scada-services-rtu-solutions/#whatarethegreatestproblemswithscadasystems?>
5. <https://www.forcepoint.com/cyber-edu/scada-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	Practical/Oral	Tutorial	Total
CSDO7021	Cyber security 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					
CSDO7021	Cyber security Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
The course aims:	
1	Introduce students to the field of cyber security management and its importance in today's digital age.
2	Help students understand the different types of cyber security threats and vulnerabilities and how they can be mitigated.
3	Teach students how to evaluate cyber security risks and develop risk management strategies.
4	Provide students with an understanding of various cyber security technologies and tools, and how they can be used to secure information systems and networks.
5	Develop students' skills in incident response planning and execution.
6	Educate students on the ethical and legal implications of cyber security management.

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 the fundamental concepts and principles of cyber security management.	L1, L2, L3
2	Analyze different types of cyber security threats and vulnerabilities.	L1, L2, L4
3	Evaluate cyber security risks and identify appropriate countermeasures.	L1, L2, L3
4	Apply best practices for securing information systems and networks.	L1, L2, L3
5	Develop and implement effective incident response plans.	L1, L2, L3
6	Understand the ethical and legal implications of cyber security management.	L1, L2

Prerequisite: Introduction to Cyber Security.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic of Ethical Hacking, Networking device and OSI layers	02	-
I	Introduction to cyber security	Concepts: Defining Cyberspace and Cybersecurity, Architecture of cyberspace, Basic concepts of information security, Types of cyber threats, Security issues and challenges of Cybersecurity, Security policies and standards, Security risk management, Security awareness and training, Risk management frameworks and Security governance Self-learning Topics: NIST Cybersecurity Framework, ISO/IEC 27001 standard, SANS Security	06	CO1
II	Tools and technologies for Cyber Security	Concepts: Access control and authentication mechanisms, Network security, Application security, Incident response and management, Firewalls and Antivirus: Significance of host firewall and Antivirus, Management of host firewall and Antivirus, Intrusion detection/prevention systems, Encryption and decryption techniques, Security testing and assessment, Threat modeling and vulnerability assessment, Cyber Security best practices, Wi-Fi security, Configuration of basic security policy and permissions. Self-learning Topics: SANS Institute reading room, MITRE ATT&CK Framework, Cybersecurity and Infrastructure Security Agency (CISA) publications.	10	CO2
III	Cyber security risks and vulnerabilities .	Courses: Human factors in security breaches, social engineering attacks, Web application security, Cloud security, Mobile device security, Internet of Things (IoT) security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, Threat modeling, Vulnerability scanning, Penetration testing, Risk assessment, Business impact analysis Self-learning Topics: Open Web Application Security Project (OWASP) Risk Assessment Methodology, Penetration Testing Execution Standard (PTES), Open-Source Security Testing Methodology Manual (OSSTMM), SANS Risk Management resources	8	CO3
IV	Implementation of Security management	Courses: Human-computer interaction (HCI) design principles, Usability testing and evaluation, User-centered design methodologies, Privacy and data protection regulations, Security by design and by default, Security architecture and design, Security engineering, Secure coding practices, Security testing, Security operations Self-learning Topics: SANS Secure Coding resources, Building Security in Maturity Model (BSIMM), Microsoft Security Development Lifecycle (SDL)	6	CO4
V	Cyber security Management Compliance and Governance	Cyber security Plan- cyber security policy, cyber crisis management plan, Security reporting and metrics Business continuity, Risk assessment, Types of security controls and their goals, Cyber Security audit and compliance, National cyber security policy and strategy, Crisis communications, Vendor and third-party management Self-learning Topics: Information Security Forum (ISF) publications, Carnegie Mellon's Computer Emergency Response Team (CERT)	06	CO5

		resources, Cybersecurity and Infrastructure Security Agency (CISA) training and resources		
VI	Emerging threats in Cyber security	Advanced persistent threats (APTs), Insider threats, Cyber Crime in various industry: Banking and Healthcare, Cybersecurity law and regulation, Cyber security aspects related to new technologies- AI/ML, IoT, Blockchain, Self-learning Topics: FireEye Threat Intelligence, resources, SANS Newsletters and Podcasts, DarkReading.com, Cloud Security Alliance research and publications	03	CO6

Textbooks:

1. Cybersecurity Management, An Organizational and Strategic Approach, Nir Kshetri, University of Toronto Press, Toronto Buffalo London, 2021.
2. Cyber Security, Incident Management Guide, Centre for Cyber Security Belgium
3. Information Security Management Handbook Sixth Edition VOLUME 2.
4. Handbook Of System, Safety and Security, Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.
5. Strategic Cyber Security Management, Peter Trim and Yang-Im Lee, by Routledge 2023.

References Books:

1. Cybersecurity and Cyberwar: What Everyone Needs to Know by P.W. Singer and Allan Friedman
2. Cybersecurity: The Essential Body of Knowledge by Dan Shoemaker, Wm. Arthur Conklin, Gregory White, Dwayne Williams, and Chuck Cothren
3. Managing Risk and Information Security: Protect to Enable by Malcolm W. Harkins
4. Security Metrics: Replacing Fear, Uncertainty, and Doubt by Andrew Jaquith
5. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) by Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak

Online References:

1. <https://www.nist.gov/cyberframework>
2. Cybersecurity and Infrastructure Security Agency (CISA): <https://www.cisa.gov/cybersecurity>
3. Journal of Cyberpsychology, Behavior, and Social Networking: <https://www.liebertpub.com/loi/cyber>
4. Cyber Security India: <https://www.cybersecurityindia.in/>
5. Center for Cyber Safety and Education: <https://www.isc2.org/Cybersecurity-Resources>

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	Practical	Tutorial	Total
CSDO7022	User Interface Design with 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					
CSDO7022	User Interface Design with Security	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives
1	To stress the importance of good interface design.
2	To understand the importance of human psychology as well as social and emotional aspect in designing good interfaces.
3	To learn the techniques of data gathering, establishing requirements, analysis and data interpretation.
4	To learn the techniques for prototyping and evaluating user experiences.
5	To understand interaction design process and bring out the creativity in each student – build innovative applications that are usable, effective and efficient for intended users.
6	To understand the role of security in User interaction design.

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 criticize bad features of interface designs.	L4
2	Predict good features of interface designs.	L5
3	Illustrate and analyze user needs and formulate user design specifications.	L4
4	Interpret and evaluate the data collected during the process.	L2, L5
5	Evaluate designs based on theoretical frameworks and methodological approaches and will be able to produce/show better techniques to improve the user interaction design interfaces.	L5
6	Evaluate designs based on cyber security aspects.	L5

Prerequisite: Basics of Cyber Security, Software Engineering concepts and any programming Language

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basics of Cyber Security, Software Engineering concepts and any programming Language Self-learning Topics: Web design languages	1	--
I	Introduction To Interaction Design	Good And Poor Design, Interaction Design, The User Experience, The Process of Interaction Design, interaction Design and The User Experience Self-learning Topics: Study of Various interactive day to day application	5	CO1
II	Understanding And Conceptualizing Interaction	Understanding The Problem Space and Conceptualizing Design, Conceptual Model, Interface Types, Cognitive Aspects, Social Interaction and The Emerging Social Phenomena, Emotions and The User Experience, Expressive And Frustrating Interfaces, Persuasive Technologies Self-learning Topics: Study of Various interactive Interface Types	5	CO2
III	Data Processing	Establishing Requirements, Five Key Issues, Techniques for Data Gathering, Data Analysis Interpretation and Presentation, Task Description and Task Analysis Self-learning Topics: Any case study of how to gather requirements. (eq.BE Project)	6	CO3
IV	Process Of Interaction Design and Design Rules and Industry Standards	Interaction Design Process, Prototyping and Conceptual Design, Interface Metaphors and Analogies, Design Principles, Principles to Support Usability, Standards And Guidelines, Golden Rules and Heuristics, ISO/IEC Standards Self-learning Topics: Study of two websites with usability concepts. Study experiments on industry standards and design principles. principles. https://xd.adobe.com/ideas/career-tips/15-rules-every-ux-designer-know/	7	CO4
V	Evaluation Techniques and Framework	The Why, what, Where and When of Evaluation, Types Of Evaluation, Case Studies DECIDE Framework, Usability Testing, Conducting Experiments, Field Studies, Heuristic Evaluation and Walkthroughs, Predictive Models. Self-learning Topics: Evaluation of any GUI with usability principles.	7	CO5
VI	Usability Design and Evaluation for Privacy and Security Solutions and Secure Systems	Usability in the Software and Hardware Life Cycle: Unique Aspects of HCI and Usability in the Privacy and Security Domain, Usability in Requirements, Usability in Design and Development, Usability in Post release, Guidelines and Strategies for Secure Interaction Design, Design Guidelines, Authorization, Communication, Design Strategies, Security by Admonition and Security by Designation, Applying the Strategies to Everyday Security Problems, Fighting Phishing at the User Interface Self-learning Topics: Any case study of how to check Cyber Security Guidelines (eg. BE Project)	8	CO6

Textbooks:

1. Interaction Design, by J. Preece, Y. Rogers and H. Sharp. ISBN 0-471-49278-7.
2. Security and Usability by Lorrie Faith Cranor, Simson Garfinkel, Publisher(s): O'Reilly Media, Inc. ISBN: 9780596553852 (Chapter 4, 13 & 14)
3. Jeff Johnson, "Designing with the mind in mind", Morgan Kaufmann Publication.
4. Wilbert O. Galitz, "The Essential Guide to User Interface Design", John Wiley & Sons, Second Edition 2002.
5. Human Computer Interaction, by Alan Dix, Janet Finlay, Gregory D Abowd, Russell Beale
6. Alan Cooper, Robert Reimann, David Cronin, "About Face3: Essentials of Interaction design", Wiley publication.
7. Wilbert O. Galitz, "The Essential Guide to User Interface Design", Wiley publication.

References:

1. Nilakshi Jain, Dhanajay R kalbande UI DESIGN: Key to Captivate User Understanding, STBGEN Learning
2. The UX Book, by Rex Hartson and Pardha S Pyla.
3. Donald A. Norman, "The design of everyday things", Basic books.

Online References:

1. https://onlinecourses.nptel.ac.in/noc21_ar05/preview
2. <https://nptel.ac.in/courses/124/107/124107008/>
3. <https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-ar10/>
4. <https://nptel.ac.in/courses/107/103/107103083/>
5. <https://www.youtube.com/watch?v=6C2Ye1makdY&list=PLW-zSkCnZ-gD5TDfs1eL5EnH2mQ0f9g6B>
6. <https://xd.adobe.com/ideas/process/>

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
CSDO7023	MANET	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					
CSDO7023	MANET	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To identify and distinguish major issues associated with ad-hoc networks.
2	To analyze the basic concepts for designing a routing protocol for MANETs.
3	To explore and analyze routing protocols of Ad-hoc network.
4	To learn the concepts of Transport layer and Security issues for MANETs.
5	To apply fundamental principles characteristics of QoS and understand the need of Energy Management in wireless ad-hoc network.
6	To learn enhancements and challenges required in securing MANET protocols

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 fundamentals of Mobile ad-hoc Networks.	L1, L2
2	Understand and be able to use advanced concept of MAC layer protocols more effectively.	L1, L2
3	Analyze different routing technologies for designing a routing protocol.	L1, L2, L3, L4
4	Understand the concepts of Transport layer and security features of Ad-hoc network.	L1, L2
5	Create the awareness of QoS and Energy Management in Ad hoc network.	L6
6	Understand the Security issues in MANET	L2, L3, L4

Prerequisite: Wireless Technology.

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Fundamentals of Wireless Communication, Wireless Metropolitan and Local Area Networks: IEEE 802.16 (WiMax) – Mesh mode, Wireless Network Security: Security in GSM; UMTS Security; Bluetooth Security; WEP.	02	--
I	Introduction to Ad-hoc Wireless Networks and IEEE 802.11	IEEE 802.11(Wi-Fi) – Architecture, Wireless Ad hoc Networks: WPAN Device Architecture, Wireless Sensor Network Applications, Advantages and Limitations Introduction: Cellular and Ad Hoc Wireless Networks, Applications of Ad Hoc Wireless Networks, Issues In Ad Hoc Wireless Networks: Medium Access Scheme, Routing, Multicasting, Transport Layer Protocols, Pricing, Quality of Service Provisioning, Addressing and Service Discovery, Energy Management, Scalability, Deployment Considerations, Ad Hoc Wireless Internet. Self-learning Topics: Global Mobile Ad Hoc Network Market	07	CO1
II	Medium Access Control Protocols	Issues in Designing a MAC Protocol, Design Goals of MAC Protocols, Classification of MAC protocols, Contention-Based Protocols with Reservation Mechanisms and Scheduling Mechanisms, IEEE 802.11a and Hiper Lan standard. Self-learning Topics: MAC Protocols that use Directional Antennas and Other MAC Protocols	06	CO2
III	Routing Protocols	Routing Protocols in Ad-hoc Wireless Networks: Introduction, Design Issues, Classification of Routing Protocols: Routing information update mechanism, Use of temporal information for routing, Routing topology, Utilization of specific resources, Multicast Routing in Ad-hoc Wireless Networks: Introduction, Design Issues, Operation of Multicast Routing Protocols, An Architecture Reference Model for Multicast Routing Protocols Self-learning Topics: Table Driven Routing Protocols, Classifications of Multicast Routing Protocols	08	CO3
IV	Transport Layer and Security Protocols	Transport Layer in Ad-hoc Wireless Networks: Introduction, Design Issues and Goals of a Transport Layer Protocol; Classification of Transport Layer Solutions. Security in Ad-hoc Wireless Networks: Issues and Challenges in Security Provisioning, Network Security Attacks classification. Self-learning Topics: TCP over Transport Layer Solutions, Key Management and Secure Touting	07	CO4
V	Quality of Service and Energy Management	Quality of Service in Ad-hoc Wireless Networks: Introduction, Issues and Challenges in Providing QoS in Ad-hoc Wireless Networks, Classification of QoS Solutions Energy Management in Ad-hoc Wireless Networks: Introduction, Need for Energy Management in Ad-hoc Wireless Networks, Classification of Energy Management Schemes Self-learning Topics: MAC Layer Solutions, Battery Management Schemes	05	CO5

VI	Securing MANET	Introduction: Threats and Challenges, Trust Management. Secure Routing: Secure routing protocol (SRP), Neighbour lookup protocol (NLP), Basic route discovery procedure, priority-based query handling, route maintenance procedure, SRP extension. Secure Data Forwarding: Secure message transmission protocol.	04	CO6
----	----------------	--	----	-----

Text Books:

1. C. S. Ram Murthy, B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall of India, 2nd Edition, 2005
2. C. K. Toh, "Adhoc Mobile Wireless Networks", Pearson Education, 2002
3. Wireless Communications & Networks, By William Stallings, Second Edition, Pearson Education

References Books:

1. Shih-Lin Wu Yu-Chee Tseng, "Wireless Ad Hoc Networking: Personal-Area, Local-Area, and the Sensory-Area Networks", Auerbach Publications, 2007
2. Subir Kumar Sarkar, "Adhoc Mobile Wireless Network: Principles, Protocols and Applications" CRC Press
3. Prashant Mohapatra and Sriramamurthy, "Ad Hoc Networks: Technologies and Protocols", Springer International Edition, 2009
4. Mohammad Ilyas," AD HOC Wireless Networks: CRC PRESS

Online References:

1. <https://www.cousera.org>
2. <https://nptel.ac.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.



Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSDO7024	Information retrieval system	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					
CSDO7024	Information retrieval system	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To learn the fundamentals of the information retrieval system.
2	To classify various Information retrieval models.
3	To demonstrate the query processing techniques and operations
4	To compare the relevance of query languages for text and multimedia data
5	To evaluate the significance of various indexing and searching techniques for information retrieval
6	To develop an effective user interface for information retrieval.

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 and describe the objectives of the basic concepts of the Information retrieval system.	L1, L2
2	Evaluate the taxonomy of different information retrieval models	L5
3	Try to solve and process text and multimedia retrieval queries and their operations.	L3
4	Evaluate text processing techniques and operations in the information retrieval system.	L5
5	Demonstrate and evaluate various indexing and searching techniques.	L3, L5

6	Design the user interface for an information retrieval system.	L6
---	--	----

Prerequisite: Data Structure

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Indexing and searching Algorithms	2	--
I	Introduction	Motivation, Basic Concepts, The Retrieval Process, Information System: Components, parts and types on information system; Definition and objectives on information retrieval system, Information versus Data Retrieval. Search Engines and browsers Self-learning Topics: Search Engines, Search API	6	CO1
II	IR Models	Modeling: Taxonomy of Information Retrieval Models, Retrieval: Formal Characteristics of IR models, Classic Information Retrieval, Alternative Set Theoretic models, Probabilistic Models, Structured text retrieval Models, models for Browsing. Self-learning Topics: Terrier	6	CO2
III	Query Processing and Operations	Query Languages: Keyword based Querying, Pattern Matching, Structural Queries, Query Protocols; Query Operations: User relevance feedback, Multimedia IR models: Data Modeling. Self-learning Topics: Proximity Queries and Wildcard Queries	6	CO3
IV	Text Processing	Text and Multimedia languages and properties: Metadata, Markup Languages, Multimedia; Text Operations: Document Preprocessing, Document Clustering. Self-learning Topics: Digital Library: Greenstone	6	CO4
V	Indexing and searching	Inverted files, other indices for text, Boolean Queries, Sequential Searching, Pattern Matching, Structural Queries, Compression; Multimedia IR: Indexing and Searching: - A Generic Multimedia indexing approach, Automatic Feature extraction; Searching Web: Challenges, Characterizing the web, Search Engines. Browsing, Meta searches, Searching using Hyperlinks. Self-learning Topics: Koha	7	CO5
VI	User Interface and Visualization	Human Computer interaction, the information access process, starting points, query specifications, context, using relevance judgments, interface support for the search process. Self-learning Topics: SeeSoft	6	CO6

Textbooks:

1. Modern Information Retrieval, Ricardo Baeza-Yates, Berthier Ribeiro- Neto, ACM Press- Addison Wesley.
2. Information Retrieval Systems: Theory and Implementation, Gerald Kowaski, Kluwer Academic Publisher.
3. Storage Network Management and Retrieval by Dr. Vaishali Khairnar, Nilima Dongre, Wiley India.

References:

1. Introduction to Information Retrieval by Christopher D. Manning and Prabhakar Raghavan, Cambridge University Press.
2. Information Storage & Retrieval by Robert Korfhage – John Wiley & Sons
3. Introduction to Modern Information Retrieval. G.G. Chowdhury. Neal Schuman.

Online References:

1. <https://www.geeksforgeeks.org/what-is-information-retrieval/>
2. <https://nlp.stanford.edu/IR-book/>
3. https://en.wikipedia.org/wiki/Information_retrieval
4. <https://people.ischool.berkeley.edu/~hearst/irbook/10/node1.html>

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
ILO7011	Product Lifecycle 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					
ILO7011	Product Lifecycle Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To familiarize the students with the need, benefits and components of PLM
2	To acquaint students with Product Data Management & PLM strategies
3	To give insights into new product development program and guidelines for designing and developing a product
4	To familiarize the students with Virtual Product Development

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	Gain knowledge about phases of PLM, PLM strategies and methodology for PLM feasibility study and PDM implementation	L1
2	Illustrate various approaches and techniques for designing and developing products	L3, L4
3	Apply product engineering guidelines / thumb rules in designing products for moulding, machining, sheet metal working etc.	L3
4	Acquire knowledge in applying virtual product development tools for components, machining and manufacturing plant.	L3

Module	Detailed Contents	Hrs
01	Introduction to Product Lifecycle Management (PLM): Product Lifecycle Management (PLM), Need for PLM, Product Lifecycle Phases, Opportunities of Globalization, Pre-PLM Environment, PLM Paradigm, Importance & Benefits of PLM, Widespread Impact of PLM, Focus and Application, A PLM Project, Starting the PLM Initiative, PLM Applications PLM Strategies: Industrial strategies, Strategy elements, its identification, selection and implementation, Developing PLM Vision and PLM Strategy, Change management for PLM	10
02	Product Design: Product Design and Development Process, Engineering Design, Organization and Decomposition in Product Design, Typologies of Design Process Models, Reference Model, Product Design in the Context of the Product Development Process, Relation with the Development Process Planning Phase, Relation with the Post design Planning Phase, Methodological Evolution in Product Design, Concurrent Engineering, Characteristic Features of Concurrent Engineering, Concurrent Engineering and Life Cycle Approach, New Product Development (NPD) and Strategies, Product Configuration and Variant Management, The Design for X System, Objective Properties and Design for X Tools, Choice of Design for X Tools and Their Use in the Design Process	09
03	Product Data Management (PDM): Product and Product Data, PDM systems and importance, Components of PDM, Reason for implementing a PDM system, financial justification of PDM, barriers to PDM implementation	05
04	Virtual Product Development Tools: For components, machines, and manufacturing plants, 3D CAD systems and realistic rendering techniques, Digital mock-up, Model building, Model analysis, Modeling and simulations in Product Design, Examples/Case studies	05
05	Integration of Environmental Aspects in Product Design: Sustainable Development, Design for Environment, Need for Life Cycle Environmental Strategies, Useful Life Extension Strategies, End-of-Life Strategies, Introduction of Environmental Strategies into the Design Process, Life Cycle Environmental Strategies and Considerations for Product Design	05
06	Life Cycle Assessment and Life Cycle Cost Analysis: Properties, and Framework of Life Cycle Assessment, Phases of LCA in ISO Standards, Fields of Application and Limitations of Life Cycle Assessment, Cost Analysis and the Life Cycle Approach, General Framework for LCCA, Evolution of Models for Product Life Cycle Cost Analysis	05

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.

REFERENCES:

1. John Stark, "Product Lifecycle Management: Paradigm for 21st Century Product Realisation", Springer-Verlag, 2004. ISBN: 1852338105
2. Fabio Giudice, Guido La Rosa, Antonino Risitano, "Product Design for the environment-A life cycle approach", Taylor & Francis 2006, ISBN: 0849327229
3. Saaksvuori Antti, Immonen Anselmie, "Product Life Cycle Management", Springer, Dreamtech, ISBN: 3540257314
4. Michael Grieve, "Product Lifecycle Management: Driving the next generation of lean thinking", Tata McGraw Hill, 2006, ISBN: 0070636265



Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7012	Reliability Engineering	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					
ILO7012	Reliability Engineering	20	20	20	80	--	--	--	100

Sr. No.	Course Objectives:
The course aims:	
1	To familiarize the students with various aspects of probability theory
2	To acquaint the students with reliability and its concepts
3	To introduce the students to methods of estimating the system reliability of simple and complex systems
4	To understand the various aspects of Maintainability, Availability and FMEA procedure

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 and apply the concept of Probability to engineering problems	L1, L3
2	Apply various reliability concepts to calculate different reliability parameters	L3
3	Estimate the system reliability of simple and complex systems	L5
4	Carry out a Failure Mode Effect and Criticality Analysis	L4

Module	Detailed Contents	Hrs
01	Probability theory: Probability: Standard definitions and concepts; Conditional Probability, Baye's Theorem. Probability Distributions: Central tendency and Dispersion; Binomial, Normal, Poisson, Weibull, Exponential, relations between them and their significance. Measures of Dispersion: Mean, Median, Mode, Range, Mean Deviation, Standard Deviation, Variance, Skewness and Kurtosis.	08
02	Reliability Concepts: Reliability definitions, Importance of Reliability, Quality Assurance and Reliability, Bath Tub Curve. Failure Data Analysis: Hazard rate, failure density, Failure Rate, Mean Time to Failure (MTTF), MTBF, Reliability Functions. Reliability Hazard Models: Constant Failure Rate, linearly increasing, Time Dependent Failure Rate, Weibull Model. Distribution functions and reliability analysis.	08
03	System Reliability: System Configurations: Series, parallel, mixed configuration, k out of n structure, Complex systems.	05
04	Reliability Improvement: Redundancy Techniques: Element redundancy, Unit redundancy, Standby redundancies. Markov analysis. System Reliability Analysis – Enumeration method, Cut-set method, Success Path method, Decomposition method.	08
05	Maintainability and Availability: System downtime, Design for Maintainability: Maintenance requirements, Design methods: Fault Isolation and self-diagnostics, Parts standardization and Interchangeability, Modularization and Accessibility, Repair Vs Replacement. Availability – qualitative aspects.	05
06	Failure Mode, Effects and Criticality Analysis: Failure mode effects analysis, severity/criticality analysis, FMECA examples. Fault tree construction, basic symbols, development of functional reliability block diagram, Fault tree analysis and Event tree Analysis	05

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.

REFERENCES:

1. L.S. Srinath, "Reliability Engineering", Affiliated East-West Press (P) Ltd., 1985.
2. Charles E. Ebeling, "Reliability and Maintainability Engineering", Tata McGraw Hill.
3. B.S. Dhillon, C. Singh, "Engineering Reliability", John Wiley & Sons, 1980.
4. P.D.T. Conon, "Practical Reliability Engg.", John Wiley & Sons, 1985.
5. K.C. Kapur, L.R. Lamberson, "Reliability in Engineering Design", John Wiley & Sons.
6. Murray R. Spiegel, "Probability and Statistics", Tata McGraw-Hill Publishing Co. Ltd.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7013	Management Information System	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					
ILO7013	Management Information System	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	The course is blend of Management and Technical field.
2	Discuss the roles played by information technology in today's business and define various technology architectures on which information systems are built
3	Define and analyze typical functional information systems and identify how they meet the needs of the firm to deliver efficiency and competitive advantage
4	Identify the basic steps in systems development

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	Explain how information systems Transform Business	L2, L4, L5
2	Identify the impact information systems have on an organization	L1
3	Describe IT infrastructure and its components and its current trends	L1, L2
4	Understand the principal tools and technologies for accessing information from databases to improve business performance and decision making	L1
5	Identify the types of systems used for enterprise-wide knowledge management and how they provide value for businesses.	L1

Module	Detailed Contents	Hrs
01	Introduction To Information Systems (IS): Computer Based Information Systems, Impact of IT on organizations, Importance of IS to Society. Organizational Strategy, Competitive Advantages and IS.	4
02	Data and Knowledge Management: Database Approach, Big Data, Data warehouse and Data Marts, Knowledge Management. Business intelligence (BI): Managers and Decision Making, BI for Data analysis. and Presenting Results	7
03	Ethical issues and Privacy: Information Security. Threat to IS, and Security Controls	7
04	Social Computing (SC): Web 2.0 and 3.0, SC in business-shopping, Marketing, Operational and Analytic CRM, E-business and E-commerce – B2B B2C. Mobile commerce.	7
05	Computer Networks Wired and Wireless technology, Pervasive computing, Cloud computing model.	6
06	Information System within Organization: Transaction Processing Systems, Functional Area Information System, ERP and ERP support of Business Process. Acquiring Information Systems and Applications: Various System development life cycle models.	8

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.

REFERENCES:

1. Kelly Rainer, Brad Prince, Management Information Systems, Wiley
2. K.C. Laudon and J.P. Laudon, Management Information Systems: Managing the Digital Firm, 10th Ed., Prentice Hall, 2007.
3. D. Boddy, A. Boonstra, Managing Information Systems: Strategy and Organization, Prentice Hall, 2008

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7014	Design of Experiments	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					
ILO7014	Design of Experiments	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand the issues and principles of Design of Experiments (DOE)
2	To list the guidelines for designing experiments
3	To become familiar with methodologies that can be used in conjunction with experimental designs for robustness and optimization.

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	Plan data collection, to turn data into information and to make decisions that lead to appropriate action.	L6
2	Apply the methods taught to real life situations.	L3
3	Plan, analyze, and interpret the results of experiments.	L4, L6

Module	Detailed Contents	Hrs
01	Introduction Strategy of Experimentation, Typical Applications of Experimental Design Guidelines for Designing Experiments, Response Surface Methodology	06

02	Fitting Regression Models Linear Regression Models, Estimation of the Parameters in Linear Regression Models Hypothesis Testing in Multiple Regression, Confidence Intervals in Multiple Regression Prediction of new response observation, Regression model diagnostics, Testing for lack of fit	08
03	Two-Level Factorial Designs The 2^2 Design, The 2^3 Design, The General 2^k Design, A Single Replicate of the 2^k Design The Addition of Center Points to the 2^k Design, Blocking in the 2^k Factorial Design, Split-Plot Designs	07
04	Two-Level Fractional Factorial Designs The One-Half Fraction of the 2^k Design, The One-Quarter Fraction of the 2^k Design The General 2^{k-p} Fractional Factorial Design, Resolution III Designs, Resolution IV and V Designs, Fractional Factorial Split-Plot Designs	07
05	Response Surface Methods and Designs Introduction to Response Surface Methodology, The Method of Steepest Ascent Analysis of a Second-Order Response Surface, Experimental Designs for Fitting Response Surfaces	07
06	Taguchi Approach Crossed Array Designs and Signal-to-Noise Ratios, Analysis Methods, Robust design examples	04

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.

REFERENCES:

1. Raymond H. Mayers, Douglas C. Montgomery, Christine M. Anderson-Cook, Response Surface Methodology: Process and Product Optimization using Designed Experiment, 3rd edition, John Wiley & Sons, New York, 2001
2. D.C. Montgomery, Design and Analysis of Experiments, 5th edition, John Wiley & Sons, New York, 2001
3. George E P Box, J Stuart Hunter, William G Hunter, Statics for Experimenters: Design, Innovation and Discovery, 2nd Ed. Wiley
4. W J Dimond, Peactical Experiment Designs for Engineers and Scintists, John Wiley and Sons Inc. ISBN: 0-471-39054-2
5. Design and Analysis of Experiments (Springer text in Statistics), Springer by A.M. Dean, and D. T.Voss.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7015	Operation Research	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					
ILO7015	Operation Research	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	Formulate a real-world problem as a mathematical programming model.
2	Understand the mathematical tools that are needed to solve optimization problems
3	Use mathematical software to solve the proposed models.

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 theoretical workings of the simplex method, the relationship between a linear program and its dual, including strong duality and complementary slackness.	L1
2	Perform sensitivity analysis to determine the direction and magnitude of change of a model's optimal solution as the data change.	L5
3	Solve specialized linear programming problems like the transportation and assignment problems, solve network models like the shortest path, minimum spanning tree, and maximum flow problems.	L3
4	Understand the applications of integer programming and a queuing model and compute important performance measures.	L1, L2



Module	Detailed Contents	Hrs
01	Introduction to Operations Research: Introduction, , Structure of the Mathematical Model, Limitations of Operations Research Linear Programming: Introduction, Linear Programming Problem, Requirements of LPP, Mathematical Formulation of LPP, Graphical method, Simplex Method Penalty Cost Method or Big M-method, Two Phase Method, Revised simplex method, Duality, Primal – Dual construction, Symmetric and Asymmetric Dual, Weak Duality Theorem, Complimentary Slackness Theorem, Main Duality Theorem, Dual Simplex Method, Sensitivity Analysis Transportation Problem: Formulation, solution, unbalanced Transportation problem. Finding basic feasible solutions – Northwest corner rule, least cost method and Vogel's approximation method. Optimality test: the stepping stone method and MODI method. Assignment Problem: Introduction, Mathematical Formulation of the Problem, Hungarian Method Algorithm, Processing of n Jobs Through Two Machines and m Machines, Graphical Method of Two Jobs m Machines Problem Routing Problem, Travelling Salesman Problem Integer Programming Problem: Introduction, Types of Integer Programming Problems, Gomory's cutting plane Algorithm, Branch and Bound Technique. Introduction to Decomposition algorithms.	14
02	Queuing models: queuing systems and structures, single server and multi-server models, Poisson input, exponential service, constant rate service, finite and infinite population	05
03	Simulation: Introduction, Methodology of Simulation, Basic Concepts,	05
	Simulation Procedure, Application of Simulation Monte-Carlo Method: Introduction, Monte-Carlo Simulation, Applications of Simulation, Advantages of Simulation, Limitations of Simulation	
04	Dynamic programming. Characteristics of dynamic programming. Dynamic programming approach for Priority Management employment smoothening, capital budgeting, Stagecoach/Shortest Path, cargo loading and Reliability problems.	05
05	Game Theory. Competitive games, rectangular game, saddle point, minimax (maximin) method of optimal strategies, value of the game. Solution of games with saddle points, dominance principle. Rectangular games without saddle point – mixed strategy for 2 X 2 games.	05
06	Inventory Models: Classical EOQ Models, EOQ Model with Price Breaks, EOQ with Shortage, Probabilistic EOQ Model,	05

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.

REFERENCES:

1. Taha, H.A. "Operations Research - An Introduction", Prentice Hall, (7th Edition), 2002.
2. Ravindran, A, Phillips, D. T and Solberg, J. J. "Operations Research: Principles and Practice", John Willey and Sons, 2nd Edition, 2009.
3. Hiller, F. S. and Liebermann, G. J. "Introduction to Operations Research", Tata McGraw Hill, 2002.
4. Operations Research, S. D. Sharma, KedarNath Ram Nath-Meerut.
5. Operations Research, KantiSwarup, P. K. Gupta and Man Mohan, Sultan Chand & Sons.

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7016	Cyber Security and Laws	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					
ILO7016	Cyber Security and Laws	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand and identify different types of cybercrime and cyber law
2	To recognized Indian IT Act 2008 and its latest amendments
3	To learn various types of security standards compliances

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 cybercrime and its effect on the outside world.	L1
2	Interpret and apply IT law in various legal issues.	L5, L3
3	Distinguish different aspects of cyber law.	L2, L4
4	Apply Information Security Standards compliance during software design and development.	L3, L6

Module	Detailed Contents	Hrs
01	Introduction to Cybercrime: Cybercrime definition and origins of the world, Cybercrime and information security, Classifications of cybercrime, Cybercrime and the Indian ITA 2000, A global Perspective on cybercrimes.	4
02	Cyber offenses & Cybercrime: How criminal plan the attacks, Social Engg, Cyber stalking, Cybercafé and Cybercrimes, Bot nets, Attack vector, Cloud computing, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Devices-Related Security Issues, Organizational Security Policies and Measures in Mobile Computing Era, Laptops	9
03	Tools and Methods Used in Cyber line. Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks, Phishing, Identity Theft (ID Theft)	6
04	The Concept of Cyberspace E-Commerce, The Contract Aspects in Cyber Law, The Security Aspect of Cyber Law, The Intellectual Property Aspect in Cyber Law, The Evidence Aspect in Cyber Law, The Criminal Aspect in Cyber Law, Global Trends in Cyber Law, Legal Framework for Electronic Data Interchange Law Relating to Electronic Banking, The Need for an Indian Cyber Law	8
05	Indian IT Act. Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals Under the IT Act, 2000, IT Act. 2008 and its Amendments	6
06	Information Security Standard compliances SOX, GLBA, HIPAA, ISO, FISMA, NERC, PCI.	6

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.

Textbooks:

1. "Cyber Security & Cyber Laws" by Nilakshi Jain & Ramesh Menon.

REFERENCES:

1. Nina Godbole, Sunit Belapure, *Cyber Security*, Wiley India, New Delhi
2. The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi
3. The Information technology Act, 2000; Bare Act- Professional Book Publishers, New Delhi.
4. Cyber Law & Cyber Crimes By Advocate Prashant Mali; Snow White Publications, Mumbai
5. Nina Godbole, *Information Systems Security*, Wiley India, New Delhi
6. Kenneth J. Knapp, *Cyber Security & Global Information Assurance* Information Science Publishing.
7. William Stallings, *Cryptography and Network Security*, Pearson Publication
8. Websites for more information is available on : The Information Technology ACT, 2008- TIFR : <https://www.tifrh.res.in>
9. Website for more information , A Compliance Primer for IT professional : <https://www.sans.org/reading-room/whitepapers/compliance/compliance-primer-professionals-33538>

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7017	Disaster Management and Mitigation Measures	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					
ILO7017	Disaster Management and Mitigation Measures	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand physics and various types of disaster occurring around the world
2	To identify extent and damaging capacity of a disaster
3	To study and understand the means of losses and methods to overcome /minimize it.
4	To understand role of individual and various organization during and after disaster
5	To understand application of GIS in the field of disaster management
6	To understand the emergency government response structures before, during and after disaster

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	Get to know natural as well as manmade disaster and their extent and possible effects on the economy	L1
2	Plan of national importance structures based upon the previous history.	L6
3	Get acquainted with government policies, acts and various organizational structure associated with an emergency.	L1
4	Get to know the simple do's and don'ts in such extreme events and act accordingly.	L1

Module	Detailed Contents	Hrs
01	Introduction Definition of Disaster, hazard, global and Indian scenario, general perspective, importance of study in human life, Direct and indirect effects of disasters, long term effects of disasters. Introduction to global warming and climate change.	03
02	Natural Disaster and Manmade disasters: Natural Disaster: Meaning and nature of natural disaster, Flood, Flash flood, drought, cloud burst, Earthquake, Landslides, Avalanches, Volcanic eruptions, Mudflow, Cyclone, Storm, Storm Surge, climate change, global warming, sea level rise, ozone depletion. Manmade Disasters: Chemical, Industrial, Nuclear and Fire Hazards. Role of growing population and subsequent industrialization, urbanization and changing lifestyle of human beings in frequent occurrences of manmade disasters.	09
03	Disaster Management, Policy and Administration Disaster management: meaning, concept, importance, objective of disaster management policy, disaster risks in India, Paradigm shift in disaster management. Policy and administration: Importance and principles of disaster management policies, command and co-ordination of in disaster management, rescue operations-how to start with and how to proceed in due course of time, study of flowchart showing the entire process.	06
04	Institutional Framework for Disaster Management in India: Importance of public awareness, Preparation and execution of emergency management programme. Scope and responsibilities of National Institute of Disaster Management (NIDM) and National disaster management authority (NDMA) in India. Methods and measures to avoid disasters, Management of casualties, set up of emergency facilities, importance of effective communication amongst different agencies in such situations. Use of Internet and softwares for effective disaster management. Applications of GIS, Remote sensing and GPS in this regard.	06
05	Financing Relief Measures: Ways to raise finance for relief expenditure, role of government agencies and NGO's in this process, Legal aspects related to finance raising as well as overall management of disasters. Various NGO's and the works they have carried out in the past on the occurrence of various disasters, Ways to approach these teams. International relief aid agencies and their role in extreme events.	09
06	Preventive and Mitigation Measures: Pre-disaster, during disaster and post-disaster measures in some events in general Structural mapping: Risk mapping, assessment and analysis, sea walls and embankments, Bio shield, shelters, early warning and communication Non-Structural Mitigation: Community based disaster preparedness, risk transfer and risk financing, capacity development and training, awareness and education, contingency plans. Do's and don'ts in case of disasters and effective implementation of relief aids.	06

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.

REFERENCES:

1. 'Disaster Management' by Harsh K.Gupta, Universities Press Publications.
2. 'Disaster Management: An Appraisal of Institutional Mechanisms in India' by O.S.Dagur, published by Centre for land warfare studies, New Delhi, 2011.
3. 'Introduction to International Disaster Management' by Damon Copolla, Butterworth Heinemann Elsevier Publications.
4. 'Disaster Management Handbook' by Jack Pinkowski, CRC Press Taylor and Francis group.
5. 'Disaster management & rehabilitation' by Rajdeep Dasgupta, Mittal Publications, New Delhi.
6. 'Natural Hazards and Disaster Management, Vulnerability and Mitigation – R B Singh, Rawat Publications
7. Concepts and Techniques of GIS –C.P.Lo Albert, K.W. Yonng – Prentice Hall (India) Publications. (Learners are expected to refer reports published at national and International level and updated information available on authentic web sites)

Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7018	Energy Audit 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					
ILO7018	Energy Audit and Management	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To understand the importance of energy security for sustainable development and the fundamentals of energy conservation
2	To introduce performance evaluation criteria of various electrical and thermal installations to facilitate energy management.
3	To relate the data collected during performance evaluation of systems for identification of energy saving opportunities.

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	To identify and describe present state of energy security and its importance	L1, L2, L4
2	To identify and describe the basic principles and methodologies adopted in energy audit of a utility.	L1, L2, L4
3	To describe the energy performance evaluation of some common electrical installations and identify the energy saving opportunities.	L1, L2, L4
4	To describe the energy performance evaluation of some common thermal installations and identify the energy saving opportunities.	L1, L2, L4
5	To analyze the data collected during performance evaluation and recommend energy saving measures	L4

Module	Detailed Contents	Hrs
01	Energy Scenario: Present Energy Scenario, Energy Pricing, Energy Sector Reforms, Energy Security, Energy Conservation and its Importance, Energy Conservation Act- 2001 and its Features. Basics of Energy and its various forms, Material and Energy balance	04
02	Energy Audit Principles: Definition, Energy audit- need, Types of energy audit, Energy management (audit) approach-understanding energy costs, Bench marking, Energy performance, Matching energy use to requirement, maximizing system efficiencies, Optimizing the input energy requirements, Fuel and energy substitution. Elements of monitoring& targeting; Energy audit Instruments; Data and information-analysis. Financial analysis techniques: Simple payback period, NPV, Return on investment (ROI), Internal rate of return (IRR)	08
03	Energy Management and Energy Conservation in Electrical System: Electricity billing, Electrical load management and maximum demand Control; Power factor improvement, Energy efficient equipment and appliances, star ratings. Energy efficiency measures in lighting system, Lighting control: Occupancy sensors, daylight integration, and use of intelligent controllers. Energy conservation opportunities in: water pumps, industrial drives, induction motors, motor retrofitting, soft starters, variable speed drives.	10
04	Energy Management and Energy Conservation in Thermal Systems: Review of different thermal loads; Energy conservation opportunities in: Steam distribution system, Assessment of steam distribution losses, Steam leakages, Steam trapping, Condensate and flash steam recovery system. General fuel economy measures in Boilers and furnaces, Waste heat recovery, use of insulation- types and application. HVAC system: Coefficient of performance, Capacity, factors affecting Refrigeration and Air Conditioning system performance and savings opportunities.	10
05	Energy Performance Assessment: On site Performance evaluation techniques, Case studies based on: Motors and variable speed drive, pumps, HVAC system calculations; Lighting System: Installed Load Efficacy Ratio (ILER) method, Financial Analysis.	04
06	Energy conservation in Buildings: Energy Conservation Building Codes (ECBC): Green Building, LEED rating, Application of Non-Conventional and Renewable Energy Sources	03

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.

REFERENCES:

1. Handbook of Electrical Installation Practice, Geofry Stokes, Blackwell Science
2. Designing with light: Lighting Handbook, By Anil Valia, Lighting System
3. Energy Management Handbook, By W.C. Turner, John Wiley and Sons
4. Handbook on Energy Audits and Management, edited by A. K. Tyagi, Tata Energy Research Institute (TERI).
5. Energy Management Principles, C.B.Smith, Pergamon Press
6. Energy Conservation Guidebook, Dale R. Patrick, S. Fardo, Ray E. Richardson, Fairmont Press
7. Handbook of Energy Audits, Albert Thumann, W. J. Younger, T. Niehus, CRC Press
8. www.energymanagertraining.com
9. www.bee-india.nic.in.



Course Code	Course Name	Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
ILO7019	Development Engineering	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					
ILO7019	Development Engineering	20	20	20	80	--	--	--	100

Course Objectives:

Sr. No.	Course Objectives:
The course aims:	
1	To familiarise the characteristics of rural Society and the Scope, Nature and Constraints of rural Development
2	To provide an exposure to implications of 73 rd CAA on Planning, Development and Governance of Rural Areas
3	An exploration of human values, which go into making a 'good' human being, a 'good' professional, a 'good' society and a 'good life' in the context of work life and the personal life of modern Indian professionals
4	To familiarise the Nature and Type of Human Values relevant to Planning Institutions

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 understanding of knowledge for Rural Development.	L3
2	Prepare solutions for Management Issues.	L3
3	Take up Initiatives and design Strategies to complete the task	L6
4	Develop acumen for higher education and research.	L6
5	Demonstrate the art of working in group of different nature	L3
6	Develop confidence to take up rural project activities independently.	L6

Module	Contents	Hrs
1	Introduction to Rural Development Meaning, nature and scope of development; Nature of rural society in India; Hierarchy of settlements; Social, economic and ecological constraints for rural development Roots of Rural Development in India Rural reconstruction and Sarvodaya program before independence; Impact of voluntary effort and Sarvodaya Movement on rural development; Constitutional direction, directive principles; Panchayati Raj - beginning of planning and community development; National extension services.	08
2	Post-Independence rural Development Balwant Rai Mehta Committee - three tier system of rural local Government; Need and scope for people's participation and Panchayati Raj; Ashok Mehta Committee - linkage between Panchayati Raj, participation and rural development.	06
3	Rural Development Initiatives in Five Year Plans Five Year Plans and Rural Development; Planning process at National, State, Regional and District levels; Planning, development, implementing and monitoring organizations and agencies; Urban and rural interface - integrated approach and local plans; Development initiatives and their convergence; Special component plan and sub-plan for the weaker section; Micro-eco zones; Data base for local planning; Need for decentralized planning; Sustainable rural development	07
4	Post 73rd Amendment Scenario 73rd Constitution Amendment Act, including - XI schedule, devolution of powers, functions and finance; Panchayati Raj institutions - organizational linkages; Recent changes in rural local planning; Gram Sabha - revitalized Panchayati Raj; Institutionalization; resource mapping, resource mobilization including social mobilization; Information Technology and rural planning; Need for further amendments.	04
5	Values and Science and Technology Material development and its values; the challenge of science and technology; Values in planning profession, research and education Types of Values Psychological values — integrated personality; mental health; Societal values — the modern search for a good society; justice, democracy, rule of law, values in the Indian constitution; Aesthetic values — perception and enjoyment of beauty; Moral and ethical values; nature of moral judgment; Spiritual values; different concepts; secular spirituality; Relative and absolute values; Human values— humanism and human values; human rights; human values as freedom, creativity, love and wisdom	10
6	Ethics Canons of ethics; ethics of virtue; ethics of duty; ethics of responsibility. Work ethics; Professional ethics; Ethics in planning profession, research and education	04

Assessment:

Internal Assessment for 20 marks:

Consisting of **Two Compulsory Class Tests**

First test based on approximately 40% of contents and second test based on remaining contents (approximately 40% but excluding contents covered in Test I)

End Semester Examination:

The weightage of each module in end semester examination will be proportional to number of respective lecture hours mentioned in the curriculum.

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.

Reference

1. ITPI, Village Planning and Rural Development, ITPI, New Delhi
2. Thooyavan, K.R. Human Settlements: A 2005 MA Publication, Chennai
3. GoI, Constitution (73rdGoI, New Delhi Amendment) Act, GoI, New Delhi
4. Planning Commission, Five Year Plans, Planning Commission
5. Planning Commission, Manual of Integrated District Planning, 2006, Planning Commission New Delhi
6. Planning Guide to Beginners
7. Weaver, R.C., The Urban Complex, Doubleday
8. Farmer, W.P. et al, Ethics in Planning, American Planning Association, Washington.
9. How, E., Normative Ethics in Planning, Journal of Planning Literature, Vol.5, No.2, pp. 123-150
10. Watson, V. Conflicting Rationalities: -- Implications for Planning Theory and Ethics, Planning Theory and Practice, Vol. 4, No.4, pp.395 – 407

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL701	DevSecOps Lab	--	2	--	--	1	--	1

Subject Code	Subject Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL701	DevSecOps Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To understand the concept of distributed version control.
2	To familiarize myself with Jenkins, build & test software Applications & Continuous integration.
3	To understand Docker to build, ship and run containerized images.
4	To familiarize with the concept of Software Configuration Management with Continuous Monitoring.
5	To understand the basics of Application/code security testing and threat modeling.
6	To familiarize with the concept of Cloud and Infrastructure as a Code.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
On successful completion of the course students will be able to,		
1	Understand the concepts of distributed version control using GIT and GITHUB	L1
2	Apply Jenkins to Build, Deploy and Test the Software Applications	L3
3	Analyze & Illustrate the Containerization of OS images and deployment of applications over Docker	L3, L4
4	Deploy and Examine the Software Configuration management using Ansible and Continuous monitoring and alerting using Prometheus and Nagios	L4
5	Use Sonarqube and snyk to perform code quality checks and Threat Dragon to create threat models to identify threats in the system.	L3
6	Implement Terraform scripts to manage VMs on a cloud.	L3

Prerequisite: DevOps

Sr. No.	Module	Detailed Content	Hours	LO
0	Prerequisite	Concept of DevOps with related technologies which are used to Code, Build, Test, Configure & Monitor the Software Applications.	02	-
I	Version Control using GIT	To Perform Version Control on documents/files websites/ Software's using GIT & GITHUB that covers all GIT commands given in GIT cheat sheet. - To implement Version control for different files/directories using GIT - To implement version control using GITHUB to sync local GIT repositories and perform various related operations.	04	LO 1
II	Working with Jenkins	- To deploy and test Java/web/Python application on jenkins server. - To implement Jenkins pipeline using scripted/declarative pipeline - To use jenkins to deploy and run test cases for Java/Web application using Selenium/JUnit	04	LO 2
III	Containerization	- To use docker to run containers of different applications and operating Systems. - To create a custom docker image using Dockerfile and upload it to the docker hub.	04	LO 3
IV	Software Configuration Management and Continuous Monitoring	- To implement continuous deployment using Ansible - To Implement automated monitoring and alerting using Prometheus - To implement continuous monitoring using Splunk/Nagios	04	LO 4
V	Application/Code Security	- To implement Application and code security testing using snyk - To implement Static Application Security Testing using SonarQube - To implement threat models to identify threats in the system using Threat Dragon	04	LO 5

VI	Cloud and Infrastructure as a code	- To create and work with virtual machine on cloud (GCP / AWS / Azure) - To implement terraform script for deploying compute/Storage/network infrastructure on the public cloud platform (GCP / AWS / Azure)	04	LO 6
----	------------------------------------	---	----	------

Text Books:

1. Prem Kumar Ponuthorai, Jon Loeliger, Version Control with Git, 3rd Edition, O'Reilly Media.
2. John Ferguson Smart, "Jenkins, The Definitive Guide", O'Reilly Publication.
3. Karl Matthias & Sean P. Kane, Docker: Up and Running, O'Reilly Publication.
4. [Russ McKendrick](#), Learn Ansible, Pakt Publication.
5. Yevgeniy Brikman, Terraform: Up and Running, 3rd Edition, O'Reilly Publication.
6. [G. Ann Campbell](#), SonarQube in Action, First Edition, Manning publication.

References:

1. Sanjeev Sharma and Bernie Coyne, "DevOps for Dummies", Wiley Publication
2. Httermann, Michael, "DevOps for Developers", Apress Publication.
3. Joakim Verona, "Practical DevOps", Pack publication

Online references:

Sr. No.	Topic	Link
1	GIT Cheat sheet	https://www.atlassian.com/git/tutorials/atlassian-git-cheatsheet
2	Jenkins	1) https://www.javacodegeeks.com/2021/04/how-to-create-run-a-job-in-jenkins-using-jenkins-freestyle-project.html 2) https://k2lacademy.com/devops-foundation/ci-cd-pipeline-using-jenkins/
3	Docker	https://docs.docker.com/get-started/docker_cheatsheet.pdf
4	Ansible	https://docs.ansible.com/ansible/latest/index.html
5	Prometheus	https://prometheus.io/docs/introduction/overview/
6	Snyk	https://snyk.io/learn/application-security/static-application-security-testing/
7	Threatdragon	https://www.threatdragon.com/#/
8	SonarQube	https://docs.sonarqube.org/latest/
9	Terraform	https://developer.hashicorp.com/terraform/intro

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.

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL702	Web Application Security Lab	--	2	--	--	1	--	1

Subject Code	Subject Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL702	Web Application Security Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To be familiarized with web application security tools and techniques.
2	To gain knowledge of discovering and exploiting vulnerabilities in web applications.
3	To Understand workflow of web application penetration testing
4	To understand the importance of access control, authorization and authentication in secure web applications.
5	To be familiar with various client-side vulnerabilities in web application.
6	To understand the injection attacks on datastore and web server.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	To configure and install various web application security tools	L1, L2,L3
2	To identify and manage vulnerabilities of web Applications and execute mitigation plans.	L1, L2, L3
3	To perform web penetration testing and organize a checklist using burp suite.	L1, L2, L3,L4
4	To identify various attacks on access control, authorization and authentication mechanisms in web applications.	L1, L2, L3,L4
5	To Examine various client -side web application security aspects.	L1,L2,L3
6	To experiment on various injection attacks on data and server in web application	L1,L2,L3

Prerequisite: Web X**DETAILED SYLLABUS:**

Sr. No.	Module	-Detailed Content	Hours	LO Mapping
0	Prerequisite	Web application terminology- cookies, sessions,web client, server ,headers	--	--
I	Installation and Set up	1. Configuration of Burp Suite 2. Installation of Mutillidae 3. Installation of Kali Linux	02	LO1
II	Vulnerability Assessment	1. Crawling the web application using Burp Spider 2. Looking for web vulnerabilities using the scanner in Burp suite 3. Replaying web requests using the Repeater tab 4. Fuzzing web requests using the burp Intruder. 5. Categorize vulnerabilities based on their severity, following industry-standard frameworks like the Common Vulnerability Scoring System (CVSS).	04	LO2
III	Web Application Pen testing	1. Discovering hidden content with Burp Suite 2. Gather information and perform reconnaissance: a) Identify the target web application and gather relevant information such as the application's technology stack, URLs, endpoints, and any other publicly available information. b) Use open-source intelligence (OSINT) techniques to gather information about the application, its infrastructure, and potential vulnerabilities. 3. Generate HTML/XML Burp suite scan report.	06	LO3
IV	Authentication and Session management	Attacking Authentication and Session Management 1. Session Management Vulnerabilities in Mutillidae 2. Brute forcing the authentication of Mutillidae 3. Building a PHP Web Application with Cookies/Sessions 4. Third-Party Authentication	04	LO4
V	XSS and CSRF	Detecting XSS Vulnerabilities in web application 1. Perform reflected XSS attack and stored XSS attack using Mutillidae 2. Exploiting stored XSS using the header and Perform DOM XSS injection using Mutillidae Detecting CSRF Vulnerabilities in web application 1. Detect CSRF attack using Burp Suite 2. Prevent CSRF attacks in web applications using Javascript.	04	LO5
VI	Injection in web application	SQL Injection 1. Bypassing Authentication using SQL injection. 2. Extracting Data using the UNION attack 3. Blind SQL injection 4. Automating SQL injection with SQLMAP tool Extended SQLi, Protecting against SQLi, and SQLi Forensics 1. Reading Files from the Target Web Server 2. Writing Files into the Target Web Server 3. Reading from and Writing to the Target Web Server 4. Reading Database Password Hashes 5. Protecting against SQL injection 6. Investigating SQL injection attacks (SQLi Forensics)	04	LO6

Text Books:

1. Practical Web Penetration Testing by Gus khawaja, packt publication
2. Hands-On Application Penetration Testing with Burp Suite: Use Burp Suite and its features to inspect, detect, and exploit security vulnerabilities in your web by Carlos A. Lozano, Dhruv Shah and Riyaz Ahemed Walikar , Packt Publication
3. The Web Application Hacker's handbook, Defydd Stuttard, Wiley Publishing

References:

1. Professional Pen Testing for Web application, Andres andreu, wrox press
2. Mastering Modern Web Penetration Testing Paperback – 28 October 2016 by Prakhar Prasad, Packt Publication

Online References:

1. <https://www.tutorialsfreak.com/web-application-penetration-testing-tutorial/>
2. <https://hackersploit.org/web-app-penetration-testing-tutorials>

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the suggested list in syllabus.. 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
CSL703	ML & Security 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				
CSL703	ML & Security Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To identify Python tools for AI and cybersecurity
2	To get basic hands-on experience with supervised, unsupervised machine learning methods
3	To detect Email Cybersecurity Threats with AI & ML techniques.
4	To understand how to combat malware, detect spam, and fight financial fraud to mitigate cybercrimes.
5	To predict network intrusions and detect anomalies with machine learning
6	To develop tools for cyber defense using deep learning.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
On successful completion of the course students will be able to,		
1	Optimize Artificial Intelligence for Cybersecurity Arsenal	L1, L2, L3, L4
2	Use machine learning algorithms with complex datasets to implement cybersecurity concepts	L1, L2, L3
3	Identify different email threats detection strategies using AI & ML techniques	L1, L2, L3, L4
4	Analyze the ML algorithms to mitigate the malware, detect spam, and fight financial fraud	L1, L2, L3, L4
5	Perform Efficient Network Anomaly Detection Using ML techniques	L1, L2, L3
6	Verify the strength of user authentication procedures with deep learning	L1, L2, L3, L4, L5

Prerequisite: Must have completed the course on Introduction to Linear Algebra and have basic familiarity with probability theory.

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7 2. 4 GB RAM 3. 500 GB Hard disk	Python 3.4.1- Python 3.11.3 any stable version

DETAILED SYLLABUS:

Sr. No.	Detailed Content	Hours	LO Mapping
I	Programming in Python and Basics of manipulation of Data, Enter Anaconda—the data scientist's environment of choice, Playing with Jupyter Notebook, feeding your AI arsenal—where to find data and malicious samples, learn to speed up a system using Python libraries with NumPy, Scikit-learn, and CUDA	04	LO1
II	Types of Regression Models, Supervised Learning using Linear regression, Unsupervised Learning using Clustering, Simple Neural Network using Perceptron	04	LO2
III	How to detect spam with Perceptrons, Email spam detection with support vector machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes algorithm, Spam detection adopting NLP	04	LO3
IV	Fraudulent emails and spoofs, Types of email fraud, Featurization techniques that convert text-based emails into numeric values, Spam detection with logistic regression	04	LO4
V	Get hold of information, modify information, disrupt services, perform distributed denial of service to and from the server where information is stored, Exploit using malware and viruses, Privilege escalation and credential compromise	04	LO5
VI	Authentication abuse prevention, Account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition	04	LO6

Textbooks:

1. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Alessandro Parisi, Packt Publishing; 1st edition, 2019
2. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, Soma Halder, Packt Publishing; 1st edition, 2018
3. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
4. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s): Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

References:

1. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.
2. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.

3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.
4. Tom Mitchell. Machine Learning. McGraw Hill, 1997.

Online References:

1. [What Is Machine Learning in Security? - Cisco](#)
2. <https://www.mdsny.com/5-top-machine-learning-use-cases-for-security/>

MOOC Courses:

1. <https://nptel.ac.in/courses/106/106/106106139/>
2. <https://nptel.ac.in/courses/106/106/106106202/>
3. <https://www.classcentral.com/course/independent-machine-learning-security-12651>

List of Experiments/Mini-Project.

1. Implement Supervised Learning model using Linear regression.
2. Implement Unsupervised Learning model using Clustering.
3. Design and implement Simple Neural Network using Perceptron.
4. Implementation and analysis of Bayesian Spam Detector with Nltk
5. Design and implement Decision Tree Phishing Detector
6. Design a Logistic Regression based Phishing Detector
7. Perform Email spam detection using SVM.
8. Set up a Decision Tree Malware Detector
9. Implement K-means malware clustering.
10. Design and implement Random Forest Malware Classifier
11. Implementation and analysis of Gaussian Network Anomaly Detection
12. Design and implement Network Anomaly Detection model.
13. Implementation and analysis of Keystroke Detection using different classifiers.
14. Perform Malicious URL detection using linear regression model.
15. Study of SMS spam detection
16. Study of Credit card fraud detection

Term Work: Term Work shall consist of at least 10 to 12 practical's 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
CSL704	Open-Source Intelligence (OSINT) 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				
CSL704	Open-Source Intelligence (OSINT) Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
The course aims:	
1	To provide hands-on experiences for students to develop critical thinking, research skills
2	To incorporate ethical usage of OSINT tools.
3	To get familiar with OSINT framework and its usage on publicly available data.
4	To learn to use the OSINT tools for social media, Email, Image, or network analysis, websites and understand the usage for Digital Forensics.
5	To performs background/profile/corporate profile checks, corporate Open-Source Intelligence (OSINT) Assessment etc.
6	Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Gain knowledge about Open-Source Intelligence understand the threats and think critically about countermeasures.	L1, L2, L3
2	Conduct advanced searches to gather intelligence and apply advance OSINT search techniques and tools.	L1, L2, L4
3	Use OSINT tools for analysis fake news, image, video data	L1, L2, L3
4	Conduct advanced searches to gather intelligence from social media sites and understand the use of Public Records for corporate and business intelligence etc.	L1, L2
5	Gather information/metadata about Maps to performance detailed map profiling	L1, L2, L3
6	Get familiar with Technical Foot printing websites for mitigating various threats	L1, L2

Prerequisite:

1. Kali Linux Installation and VM deployment.
2. Networking and security fundamentals

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	The Evolution of Open-Source Intelligence,	Open-Source Information Categories OSINT Types, Digital Data Volume, OSINT Organizations, Parties Interested in OSINT Information, International Organizations, Information Gathering Types, Benefits of OSINT, Challenges of Open-Source Intelligence Legal and Ethical Constraints	1	LO1
I	Introduction To Online Threats and Countermeasures	Online Threats- Securing the Operating System: Hardening the Windows OS, Staying Private in Windows, Destroying Digital Traces General Privacy Settings- Avoiding Pirated Software, Handling Digital Files Metadata, Physically Securing Computing Devices	1	LO1
II	Using Search Engines to Locate Information	Search Engine Technique - Keywords Discovery and Research, - Google, Privacy-Oriented Search Engines, Other Search Engines, Business Search Sites, Metadata Search Engines, Code Search FTP Search Engines Automated Search Tools, Dorks	2	LO2
III	Searching for Digital Files	News Search - Customize Google News, News Websites, Fake News Detection - Document Search, Image, Video, File Extension and File Signature List, Productivity Tools	2	LO4
IV	People Search Engines and Public Records	Social Media Intelligence: What Is Social Media Intelligence? Social Media Content Types, General Resources for Locating Information on Social Media Sites Pastebin Sites People Search Engine, Public Records and example of Public Records, Searching for Personal Details, General People Search , Online Registries, Vital Records, Criminal and Court Search, Property Records, Tax and Financial Records, Social Security Number Search Username Check, E-mail Search and Investigation Data Compromised Repository Websites, Phone Number Search	6	LO4
V	Online Maps:	The Basics of Geolocation Tracking, How to Find the GPS Coordinates of Any Location on a Map How to Find the Geocode Coordinates from a Mailing Address, General Geospatial Research Tools Commercial Satellites, Date/Time Around the World, Location-Based social media, Conducting Location Searches on social media Using Automated Tools, Country Profile Information Transport Tracking	6	LO5
VI	Technical Foot printing:	Website History and Website Capture Website Monitoring Services - RSS Feed Investigate the Target Website, Investigate the Robots.txt File, Mirror the Target Website Extract the Links Check the Target Website's Backlinks Monitor Website Updates Check the Website's Archived Contents	6	LO6

		Identify the Technologies Used, Web Scraping Tools Investigate the Target Website's File Metadata, Website Certification Search, Website Statistics and Analytics Tools, Website Reputation Checker Tools, Passive Technical Reconnaissance Activities, WHOIS Lookup, Subdomain Discovery, DNS Reconnaissance, IP Address Tracking		
--	--	---	--	--

Textbooks:

1. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence by Nihad A. Hassan (Author), Rami Hijazi (Author)
2. OSINT Techniques - Resources for Uncovering Online Information - 10th Edition (2023) by Michael Bazzell
3. Operator Handbook: Red Team + OSINT + Blue Team Reference by Joshua Picolet

References:

1. We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News by Eliot Higgins
2. Extreme Privacy: What It Takes to Disappear in America by Michael Bazzell

Tools:

1. <https://cheatsheet.haax.fr/open-source-intelligence-osint/>
2. <https://inteltechniques.com/tools/>
3. <https://hunter.io/>
4. <https://www.shodan.io/>
<https://github.com/laramies/theHarvester>
5. <https://www.osintcombine.com/osint-bookmarks>
6. <https://osintframework.com/>
7. <https://learn.baselgovernance.org/enrol/index.php?id=79>
8. <https://inteltechniques.com/>
9. <https://www.bellingcat.com/>
10. <https://www.tracelabs.org/>

List of Experiments/Mini-Project.

Sr.No.	Detailed Content
1	• Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information. • Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization. • Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing
2	• Using OSINT tool such as (Harvester) you can gather information like emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key server.
3	• Use OSINT DORKS (create and execute search queries) to verify the accuracy of the information by cross-referencing various sources and critically evaluating the reliability and credibility of the new article.
4	• To perform the reverse Image analysis for finding physical location where the content was captured. Use OSINT tool to use image metadata, landmarks, street signs, or other visual cues to identify the geolocation accurately.

5	Using OSINT tools gather Tactical information using WHOIS lookup tools or websites like DomainTools (domain, registration details, owner's contact information, registration date, and expiration date.) Archives, Text, Reverse Image Search, Images and EXIF data, Source code, Others TLD, Mentions of target, Check info such as via RSS,SSL certificates, Robots/Sitemap, Port scans, Reverse IP lookup
6	Utilize website crawling OSINT tools to gather a comprehensive list of URLs, internal links, and structure of the website
7	Use OSINT Tools to identify the technologies and frameworks used by the website, such as content management systems (CMS), server software, programming languages, or analytics tools and create vulnerability reports.
8	Determine the geolocation (country, city, or approximate location) of each IP address (at least 10) One can use online IP geolocation tools, databases, and various techniques to gather information and accurately identify the physical location associated with each IP
9	Conduct a comprehensive OSINT investigation about well-known company and gather information about the company's history, key executives, financial data, partnerships, news mentions, and any other relevant details using online databases, news articles, corporate websites, and industry reports
10	Analyze the company's competitors to understand their market positioning, strengths, and weaknesses. Tools like SEMrush, Similar Web, or Alexa or any other OSINT tool can provide website traffic, keyword analysis, and competitor comparisons
11	Fake News detection - Analyze at least 5 OSINT tools to detect, verify, authenticate, fake news and report.
12	Example Mini Project suggestion - Digital Footprint Analysis using OSINT Tools: Assess and analyze your own digital footprints wrt, Personal Information, data (full name, age, date of birth, address, phone number, and email address), images, videos (online directories, social media profiles (at least 3 social media accounts), personal websites, Online Professional Presence and analyze. - Posts, comments, photos, and other content that they have shared publicly or with specific privacy settings. - Analyze their online interactions, connections, interests, and activities. - Analyze the nature of the content, locations, events, or people, as it can provide insights into activities, hobbies, or relationships. - Analyze work experience, educational background, skills, recommendations, and any professional associations or achievements.

Term Work: Term Work shall consist of at least 10 to 12 practical's 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
CSP701	Major Project I	--	6#	--	--	3	--	3

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSP701	Major Project I	--	--	--	--	25	25	50

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, analyzing the problem and designing solutions.

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	To develop the understanding of the problem domain through extensive review of literature.	L6
2	To Identify and analyze the problem in detail to define its scope with problem specific data.	L4
3	To know various techniques to be implemented for the selected problem and related technical skills through feasibility analysis.	L3
4	To design solutions for real-time problems that will positively impact society and environment.	L6
5	To develop clarity of presentation based on communication, teamwork and leadership skills.	L6
6	To Cultivate professional and ethical behavior.	L6

Guidelines:

- Project Topic Selection and Allocation:**

1. Project topic selection Process to be defined and followed:
2. Project orientation can be given at the end of sixth semester.
3. Students should be informed about the domain and domain experts whose guidance can be taken before selecting projects.
4. Students should be recommended to refer papers from reputed conferences/ journals like IEEE, Elsevier, ACM etc. which are not more than 3 years old for review of literature.
5. Students can certainly take ideas from anywhere but be sure that they should evolve them in a unique way to suit their project requirements. Students can be informed to refer Digital India portal, SIH portal or any other hackathon portal for problem selection.

- Topics can be finalized with respect to following criterion:

Topic Selection: The topics selected should be novel in nature (Product based, Application based, or Research based) or should work towards removing the lacuna in currently existing systems.

Technology Used: Use of the latest technology or modern tools can be encouraged.

- Students should not repeat work done previously (work done in the last three years).
- Project work must be carried out by a group of at least 2 students and a maximum of 4.
- The project work can be undertaken in a research institute or organization/Industry/any business establishment. (Out-house projects)
- The project proposal presentations can be scheduled according to the domains and should be judged by faculty who are experts in the domain.
- The head of department and senior staff along with project coordinators will take decision regarding final selection of projects.
- Guide allocation should be done, and students have to submit weekly progress reports to the internal guide.
- 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.
- In the case of industry/ out-house projects, a visit by internal guide will be preferred and external members can be called during the presentation at various levels.

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.

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
- Implementation Plan for Next Semester
- Timeline Chart for Term I and Term-II (Project Management tools can be used.)
- References

Desirable

- Students can be asked to undergo some Certification course (for the technical skill set that will be useful and applicable for projects).

Term Work:

Distribution of marks for term work shall be done based on following:

1. Weekly Log Report
2. Project Work Contribution
3. Project Report (Spiral Bound) (both side print)
4. Term End Presentation (Internal)

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

Oral and Practical:

The Oral and Practical examination (Final Project Evaluation) of Project 1 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 follows:

1. Quality of problem selected.
2. Clarity of problem definition and feasibility of problem solution
3. Relevance to the specialization / industrial trends
4. Originality
5. Clarity of objective and scope
6. Quality of analysis and design
7. Quality of written and oral presentation
8. Individual as well as teamwork



Program Structure for Fourth Year Engineering Semester VII & VIII
UNIVERSITY OF MUMBAI
 (With Effect from 2023-24)

Semester VIII

Course Code	Course Name	Teaching Scheme (Contact Hours)				Credits Assigned			
		Theory		Prac	Theory	Oral	Total		
CSC801	Malware Analysis	3		--	3	--	3		
CSDO801X	Department Optional Course – 5	3		--	3	--	3		
CSDO802X	Department Optional Course – 6	3		--	3	--	3		
CSIO801X	Institute Optional Course – 2	3		--	3	--	3		
CSL801	Mobile Forensic Lab	--		2	--	1	1		
CSL802	Dark Web Investigation Lab	--		2	--	1	1		
CSP801	Major Project II	--		12#	--	6	6		
Total		12		16	12	8	20		
Course Code	Course Name	Examination Scheme							
		Theory				Term Work	Oral	Total	
		Internal Assessment			End Sem Exam	Exam. Duration (in Hrs)			
		Test 1	Test2	Avg					
CSC801	Malware Analysis	20	20	20	80	3	--	--	100
CSDO801X	Department Optional Course – 5	20	20	20	80	3	--	--	100
CSDO802X	Department Optional Course – 6	20	20	20	80	3	--	--	100
ILO801X	Institute Optional Course – 2	20	20	20	80	3	--	--	100
CSL801	Mobile Forensic Lab	--	--	--	--	--	25	25	50
CSL802	Dark Web Investigation Lab	--	--	--	--	--	25	25	50
CSP801	Major Project II	--	--	--	--	--	100	50	150
Total		--	--	80	320	--	150	100	650

indicates workload of Learner (Not Faculty), for Major Project



Students group and load of faculty per week.

Major Project 1 and 2:

Students can form groups with minimum 2 (Two) and not more than 4 (Four) Faculty Load: In Semester VII – ½ hour per week per project group.

In Semester VIII – 1 hour per week per project group

CSDO801X	Department Optional Course – 5
CSDO8011	Social & Ethical Issues of the Internet
CSDO8012	IoTs & Embedded Security
CSDO8013	Cognitive Psychology in Cyber Security
CSDO8014	Intelligent Forensic

CSDO802X	Department Optional Course –6
CSDO8021	Advance Blockchain Technology
CSDO8022	Metaverse
CSDO8023	Green IT
CSDO8024	Cyber Security laws & legal aspects

	Institute Optional Course – 2 (Common for all branches will be notified)
ILO8011	Project Management
ILO8012	Finance Management
ILO8013	Entrepreneurship Development and Management
ILO8014	Human Resource Management
ILO8015	Professional Ethics and CSR
ILO8016	Research Methodology
ILO8017	IPR and Patenting
ILO8018	Digital Business Management
ILO8019	Environmental Management

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, <u>Secret Social Media Lives</u>, 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 (IoT): 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 \(ebooks.com\)](https://ebooks.com)
2. [Forensic Intelligence by Robert Milne \(ebook\) \(ebooks.com\)](https://ebooks.com)
3. [The impact of automation and artificial intelligence on digital forensics \(wiley.com\)](https://wiley.com)
4. [Intelligence-Led Policing: The New Intelligence Architecture \(ojp.gov\).](https://ojp.gov)
5. [How AI can be used in forensic science: Challenges and prospects — DocInsights](https://docinsights.com)

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. Reijnsbergen, 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. Sādhana 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							
		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 Compliance	• 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, Cengage Learning.
4. Gopalan, Project Management, , Wiley India
5. Dennis Lock, Project Management, Gower Publishing England, 9th Ed.

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 module 3)
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				
		Tes t1	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 in HRM.	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, 15th edition, 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 Eastern Limited.
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 module 3)
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 of India
2. Keayla B K, Patent system and related issues at a glance, Published by National Working Group on Patent Laws
3. T Sengupta, 2011, Intellectual Property Law in India, Kluwer Law International
4. Tzen Wong and Graham Dutfield, 2010, Intellectual Property and Human Development: Current Trends and Future Scenario, Cambridge University Press
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 Intellectual 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 mohd Iqbal 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 Property Rights,
12. Mathew Y Maa, 2009, Fundamentals of Patenting and Licensing for Scientists and Engineers, World Scientific Publishing Company
13. N S Rathore, S M Mathur, Priti Mathur, Anshul Rathi, IPR: Drafting, Interpretation of Patent Specifications and Claims, New India Publishing Agency
14. Vivien Irish, 2005, Intellectual Property Rights for Engineers, 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 module 3)
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 Topo 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, Vinocenzo Morabito, 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-en](https://doi.org/10.1787/9789264221796-en) OECD 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, Macmillan 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. 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. 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.



