VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELAGAVI

Scheme of Teaching and Examinations and Syllabus

M.Tech., Cyber Forensics and Information Security (SFC)

(Effective from Academic year 2020 - 21)

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21
M.Tech Cyber Forensics and Information Security (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)

I SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activity	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	PCC	20SFC11	Mathematical Foundations of Computer Science	03	--	02	03	40	60	100	4
2	PCC	20SFC12	Ethical Hacking	03	--	02	03	40	60	100	4
3	PCC	20SFC13	Pragmatic of Information Security	03	--	02	03	40	60	100	4
4	PCC	20SFC14	Cyber Crime and Cyber Forensics	03	--	02	03	40	60	100	4
5	PCC	20SFC15	Cloud Security	03	--	02	03	40	60	100	4
6	PCC	20SFCL16	Ethical Hacking Laboratory	--	04	--	03	40	60	100	2
7	PCC	20RMI17	Research Methodology and IPR	01	--	02	03	40	60	100	2
			TOTAL	**16**	**04**	**12**	**21**	**280**	**420**	**700**	**24**

Note: PCC: Profession Core

Skill development activities:

Students and course instructor/s to involve either individually or in groups to interact together to enhance the learning and application skills. The students should interact with industry (small, medium and large), understand their problems or foresee what can be undertaken for study in the form of research/ testing / projects, and for creative and innovative methods to solve the identified problem. The students shall

1. Gain confidence in modelling of systems and algorithms.
2. Work on different software/s (tools) to Simulate, analyze and authenticate the output to interpret and conclude. Operate the simulated system under changed parameter conditions to study the system with respect to thermal study, transient and steady state operations, etc.
3. Handle advanced instruments to enhance technical talent.
4. Involve in case studies and field visits/ field work.
5. Accustom with the use of standards/codes etc., to narrow the gap between academia and industry.

All activities should enhance student's abilities to employment and/or self-employment opportunities, management skills, Statistical analysis, fiscal expertise, etc.

Internship: All the students have to undergo mandatory internship of 6 weeks during the vacation of I and II semesters and /or II and III semesters. A University examination shall be conducted during III semester and the prescribed credit shall be counted for the same semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared as fail in internship course and have to complete the same during the subsequent University examination after satisfying the internship requirements.

Note: (i) Four credit courses are designed for 50 hours Teaching – Learning process.
(ii) Three credit courses are designed for 40 hours Teaching – Learning process.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21
M.Tech Cyber Forensics and Information Security (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)

II SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activity	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	PCC	20SFC21	Preserving and Recovering Digital Evidence	03	--	02	03	40	60	100	4
2	PCC	20SFC22	Operating System Security	03	--	02	03	40	60	100	4
3	PCC	20SFC23	Secured Programming	03	--	02	03	40	60	100	4
4	PEC	20SFC24X	Professional elective 1	04	--	--	03	40	60	100	4
5	PEC	20SFC25X	Professional elective 2	04	--	--	03	40	60	100	4
6	PCC	20SFCL26	Mini Project	--	04	--	03	40	60	100	2
7	PCC	20SFC27	Technical Seminar	--	02	--	--	100	--	100	2
			TOTAL	**17**	**06**	**06**	**18**	**340**	**360**	**700**	**24**

Note: PCC: Profession Core, PEC: Professional Elective Course

Professional Elective-1		**Professional Elective-2**	
Course Code 20SFC24X	**Course Title**	**Course Code 20SFC25X**	**Course Title**
20SFC241	Cyber Laws and Ethics	20SFC251	Data Mining & Data Warehousing
20SFC242	Biometric Security	20SFC252	Database Security
20SFC243	Information Security Policies in Industry	20SFC253	Enterprise Application Programming
20SFC244	Trust Management in E-commerce	20SFC254	Machine Learning Techniques

Note:

1. Technical Seminar: CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a senior faculty of the department. Participation in the seminar by all postgraduate students of the program shall be mandatory.
The CIE marks awarded for Technical Seminar, shall be based on the evaluation of Seminar Report, Presentation skill and performance in Question and Answer session in the ratio 50:25:25.

2. Internship: All the students shall have to undergo mandatory internship of 6 weeks during the vacation of I and II semesters and /or II and III semesters. A University examination shall be conducted during III semester and the prescribed internship credit shall be counted in the same semester. Internship shall be considered as a head of passing and shall be considered for the award of degree. Those, who do not take-up/complete the internship shall be declared as fail in internship course and have to complete the same during the subsequent University examination after satisfying the internship
requirements.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21
M.Tech Cyber Forensics and Information Security (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)

III SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activities	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	PCC	20SFC31	File System Forensic Analysis	03	--	02	03	40	60	100	4
2	PEC	20SFC32X	Professional elective 3	03	--	--	03	40	60	100	3
3	PEC	20SFC33X	Professional elective 4	03	--	--	03	40	60	100	3
4	Project	20SFC34	Project Work phase -1	--	02	--	--	100	--	100	2
5	PCC	20SFC35	Mini-Project	--	02	--	--	100	--	100	2
6	Internship	20SFCI36	Internship	(Completed during the intervening vacation of I and II semesters and /or II and III semesters.)			03	40	60	100	6
			TOTAL	**09**	**04**	**02**	**12**	**360**	**240**	**600**	**20**

Note: PCC: Profession Core, PEC: Professional Elective Course

Professional Elective-3		**Professional Elective-4**	
Course Code 20SFC32X	**Course Title**	**Course Code 20SFC33X**	**Course Title**
20SFC321	Security Architecture Design	20SFC331	Managing Big Data
20SFC322	Steganography and Digital Watermarking	20SFC332	Mobile Application Development
20SFC323	Mobile Device Forensics	20SFC333	Social Network Analysis
20SFC324	Security Assessment and Verification	20SFC334	Software Metrics & Quality Assurance

Note:

1. Project Work Phase-1: Students in consultation with the guide/co-guide if any, shall pursue literature survey and complete the preliminary requirements of selected Project work. Each student shall prepare relevant introductory project document and present a seminar.

CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide if any, and a senior faculty of the department. The CIE marks awarded for project work phase -1, shall be based on the evaluation of Project Report, Project Presentation skill and Question and Answer session in the ratio 50:25:25. SEE (University examination) shall be as per the University norms.

2. Internship: Those, who have not pursued /completed the internship shall be declared as fail in internship course and have to complete the same during subsequent University examinations after satisfying the internship requirements. Internship SEE (University examination) shall be as per the University norms.

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI
Scheme of Teaching and Examinations – 2020 - 21
M.Tech Cyber Forensics and Information Security (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)

IV SEMESTER

SL. No.	Course	Course Code	Course Title	Teaching Hours / Week			Examination				Credits
				Theory	Practical / Seminar	Skill Development Activity	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
1	Project	20SFC41	Project work phase 2	--	04	03	03	40	60	100	20
			TOTAL	**--**	**04**	**03**	**03**	**40**	**60**	**100**	**20**

Note:
Project Work Phase-2:
CIE marks shall be awarded by a committee comprising of HoD as Chairman, Guide/co-guide, if any, and a Senior faculty of the department. The CIE marks awarded for project work phase -2, shall be based on the evaluation of Project Report subjected to plagiarism check, Project Presentation skill and Question and Answer session in the ratio 50:25:25.

SEE shall be at the end of IV semester. Project work evaluation and Viva-Voce examination (SEE), after satisfying the plagiarism check, shall be as per the University norms.

M.TECH IN NETWORK AND INTERNET ENGINEERING (LNI)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER -I

MATHEMATICAL FOUNDATION OF COMPUTER SCIENCE

Course Code	20LNI11, 20SCS11, 20SCE11, 20SFC11, 20SCN11, 20SSE11, 20SIT11, 20SAM11, 20SIS11	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Vector Spaces: Vector spaces; subspaces Linearly independent and dependent vectors Basis and dimension; coordinate vectors-Illustrative examples. Linear transformations, Representation of transformations by matrices;
(RBT Levels: **L1 & L2)** (Textbook:1)

Module-2

Orthogonality and least squares: Inner product, orthogonal sets, orthogonal projections, orthogonal bases. Gram-Schmidt orthogonalization process. QR factorizations of a matrices, least square problems, applications to linear models (least square lines and least square fitting of other curves).
(RBT Levels: **L2 & L3)** (Textbook:1)

Module-3

Symmetric and Quadratic Forms: Diagonalization, Quadratic forms, Constrained Optimization, The Singular value decomposition. Applications to image processing and statistics, Principal Component Analysis
(RBT Levels: **L2 & L3)** (Textbook:1)

Module-4

Statistical Inference: Introduction to multivariate statistical models: Correlation and Regression analysis, Curve fitting (Linear and Non-linear)
(RBT Levels: **L2 & L3)** (Textbook:3)

Module-5

ProbabilityTheory: Random variable (discrete and continuous), Probability mass function (pmf), Probability density function (pdf), Mathematical expectation, Sampling theory: testing of hypothesis by ***t***-test, χ^2- test.
(RBT Levels: **L1 & L2)** (Textbook:3)

Course Outcomes:

On completion of this course, students are able to:

1. Understand the numerical methods to solve and find the roots of the equations.
2. Apply the technique of singular value decomposition for data compression, least square approximation in solving inconsistent linear systems
3. Understand vector spaces and related topics arising in magnification and rotation of images.
4. Utilize the statistical tools in multi variable distributions.
5. Use probability formulations for new predictions with discrete and continuous RV's.

Question Paper Pattern:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.
- The question paper will have ten full questions carrying equal marks.
- Each full question consisting of 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbooks:

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Linear Algebra and its Applications	David C. Lay, Steven R. Lay and J. J. McDonald	Pearson Education Ltd	5th Edition 2015.
2	Numerical methods for Scientific and Engg. Computation	M K Jain, S.R.K Iyengar, R K. Jain	New Age International	6th Ed., 2014

3	Probability, Statistics and Random Process	T. Veerarajan	Tata Mc-Graw Hill Co	3rd Edition 2016
Reference books:				
Sl No	**Title of the book**	**Name of the Author/s**	**Publisher Name**	**Edition and year**
1	Optimization: Theory & Applications Techniques	Rao. S.S	Wiley Eastern Ltd New Delhi.	
2	Signals, Systems, and Inference	Alan V. Oppenheim and George C. Verghese	Spring	2010.
3	Foundation Mathematics for Computer Science	John Vince	Springer International	
4	Higher Engineering Mathematics	B.S. Grewal	Khanna Publishers	44th Ed.,2017

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER -I

ETHICAL HACKING

Course Code	**20SFC12**	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.

Module 2

Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access, After hacking root.

Module 3

Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.

Module 4

Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS.

Module 5

Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

Course outcomes:
At the end of the course the student will be able to:

- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Explain aspects of security, importance of data gathering, foot printing and system hacking.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.
- Demonstrate how intruders escalate privileges.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to

60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Hacking Exposed 7: Network Security Secrets & Solutions	Stuart McClure, Joel Scambray and Goerge Kurtz	Tata McGraw Hill Publishers	2010
2	Microsoft Windows Security Resource Kit	Bensmith, and Brian Komer	Prentice Hall of India	2010
Reference Books				
1	Hacking Exposed Network Security Secrets & Solutions	Stuart McClure, Joel Scambray and Goerge Kurtz	Tata McGraw Hill Publishers	5th Edition2010
3	Gray Hat Hacking The Ethical Hackers Handbook	Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle	McGraw-Hill Osborne Media paperback	3rd Edition,2011

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER -I

PRAGMATIC OF INFORMATION SECURITY

Course Code	**20SFC13**	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Overview: Computer Security Concepts, Requirements, Architecture, Trends, Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots Case Study: Readings, Intrusion and intrusion detection by John McHugh.

Module 2

User Authentication: Password, Password-based, token based, Biometric, Remote User authentication. Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control Internet Authentication Applications: Kerberos, X.509, PKI, Federated Identity Management.

Module 3

Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers. Symmetric Encryption and Message Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution.

Module 4

Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham.

Module 5

Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots, Rootkits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks Case Study.

Course outcomes:

At the end of the course the student will be able to:

- Explain the fundamentals of Cryptographic techniques.
- Identify the security issues in the network and resolve it.
- Implement security algorithms in the field of Information technology
- Identifying the type of malware attacks and implementing preventive measures.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Computer Security: Principles and Practice	William Stalling &Lawrie	Pearson.	2010
Reference Books				
1	Readings: Smashing The Stack For Fun And Profit	Aleph	http:// www.phrack.com/	
2	Computer Security Fundamentals	Chuck Easttom	Pearson	2012

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER -I

CYBER CRIME AND CYBER FORENSICS

Course Code	**20SFC14**	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime, Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

Module 2

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

Module 3

Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

Module 4

Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

Module 5

Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

Course outcomes:
At the end of the course the student will be able to:

- Explain the fundamentals and types of cybercrime.
- Distinguish various types of computer crime.
- Illustrate computer forensic techniques to identify the digital forensics associated with criminal activities.
- Apply forensic analysis tools to recover important evidence for identifying computer crime.
- Discuss laws and ethics involved in cyber crime.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cybercrime	Bernadette H Schell, Clemens Martin	ABC – CLIO Inc, California,	2004
2	Understanding Forensics in IT		NIIT Ltd	2005
3	Computer Forensics and Investigations	Nelson Phillips and EnfingerSteuart	Cengage Learning	2009
Reference Books				
1	Incident Response and Computer Forensics	Kevin Mandia, Chris Prosise, Matt Pepe	Tata McGraw -Hill	2006
2	Software Forensics	Robert M Slade	Tata McGraw - Hill	2005

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER -I

CLOUD SECURITY

Course Code	**20SFC15**, 20LNI333, 20SCE331	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.

Module 2

Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.

Module 3

Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).

Module 4

Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.

Module 5

Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations. Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.

Course outcomes:
At the end of the course the student will be able to:

- Demonstrate the growth of Cloud computing, architecture and different modules of implementation.
- Evaluate the different types of cloud solutions among IaaS, PaaS, SaaS.
- Access the security implementation flow, actions and responsibilities of stake holders.
- Generalize the Data Centre operations, encryption methods and deployment details.
- Provide recommendations for using and managing the customer's identity and choose the type of virtualization to be used.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance	Tim Mather, SubraKumaraswamy , ShahedLatif	Oreilly Media	2009
Reference Books				
1	Securing the Cloud, Cloud Computer Security Techniques and Tactics	Vic (J.R.) Winkler	Syngress	2011

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER – I

ETHICAL HACKING LABORATORY

Course Code	**20SFCL16**	CIE Marks	40
Teaching Hours/Week (L:P:S)	0:4:0	SEE Marks	60
Credits	02	Exam Hours	03

List of Experiments

1. Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network.
2. LOIC: DoS attack using LOIC.
3. FTK: Bit level forensic analysis of evidential image and reporting the same.
4. Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network. 4.
5. HTTrack: Website mirroring using Httrack and hosting on a local network.
6. XSS: Inject a client side script to a web application.
7. Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.

Course outcomes:
At the end of the course the student will be able to:

- Evaluate modern tools
- Analyze packet capturing in network
- Define forensic analysis
- Security in various web applications

Conduction of Practical Examination:
All laboratory experiments (nos) aretobeincludedforpracticalexamination.

Studentsare allowed to pick one experimentfrom **the list** Strictlyfollow theinstructions as printed on the cover page of answer script for breakup of marks **Change of experiment is allowed only once and marks allotted to the procedure part to be made zero.**

RESEARCH METHODOLOGY AND IPR			
Course Code	20RMI17	CIE Marks	40
Teaching Hours/Week (L:P:SDA)	1:0:2	SEE Marks	60
Credits	02	Exam Hours	03

Module-1
Research Methodology: Introduction, Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Importance of Knowing How Research is Done, Research Process, Criteria of Good Research, and Problems Encountered by Researchers in India. **Defining the Research Problem:** Research Problem, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem, An Illustration.
Module-2
Reviewing the literature: Place of the literature review in research, Bringing clarity and focus to your research problem, Improving research methodology, Broadening knowledge base in research area, Enabling contextual findings, How to review the literature, searching the existing literature, reviewing the selected literature, Developing a theoretical framework, Developing a conceptual framework, Writing about the literature reviewed. **Research Design:** Meaning of Research Design, Need for Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Designs, Basic Principles of Experimental Designs, Important Experimental Designs.
Module-3
Design of Sampling: Introduction, Sample Design, Sampling and Non-sampling Errors, Sample Survey versus Census Survey, Types of Sampling Designs. **Measurement and Scaling:** Qualitative and Quantitative Data, Classifications of Measurement Scales, Goodness of Measurement Scales, Sources of Error in Measurement Tools, Scaling, Scale Classification Bases, Scaling Technics, Multidimensional Scaling, Deciding the Scale. **Data Collection**: Experimental and Surveys, Collection of Primary Data, Collection of Secondary Data, Selection of Appropriate Method for Data Collection, Case Study Method.
Module-4
Testing of Hypotheses: Hypothesis, Basic Concepts Concerning Testing of Hypotheses, Testing of Hypothesis, Test Statistics and Critical Region, Critical Value and Decision Rule, Procedure for Hypothesis Testing, Hypothesis Testing for Mean, Proportion, Variance, for Difference of Two Mean, for Difference of Two Proportions, for Difference of Two Variances, P-Value approach, Power of Test, Limitations of the Tests of Hypothesis. **Chi-square Test:** Test of Difference of more than Two Proportions, Test of Independence of Attributes, Test of Goodness of Fit, Cautions in Using Chi Square Tests.
Module-5

Interpretation and Report Writing: Meaning of Interpretation, Technique of Interpretation, Precaution in Interpretation, Significance of Report Writing, Different Steps in Writing Report, Layout of the Research Report, Types of Reports, Oral Presentation, Mechanics of Writing a Research Report, Precautions for Writing Research Reports.

Intellectual Property: The Concept, Intellectual Property System in India, Development of TRIPS Complied Regime in India, Patents Act, 1970, Trade Mark Act, 1999,The Designs Act, 2000, The Geographical Indications of Goods (Registration and Protection) Act1999, Copyright Act,1957,The Protection of Plant Varieties and Farmers' Rights Act, 2001,The Semi-Conductor Integrated Circuits Layout Design Act, 2000, Trade Secrets, Utility Models, IPR and Biodiversity, The Convention on Biological Diversity (CBD) 1992, Competing Rationales for Protection of IPRs, Leading International Instruments Concerning IPR, World Intellectual Property Organisation (WIPO),WIPO and WTO, Paris Convention for the Protection of Industrial Property, National Treatment, Right of Priority, Common Rules, Patents, Marks, Industrial Designs, Trade Names, Indications of Source, Unfair Competition, Patent Cooperation Treaty (PCT), Advantages of PCT Filing, Berne Convention for the Protection of Literary and Artistic Works, Basic Principles, Duration of Protection, Trade Related Aspects of Intellectual Property Rights(TRIPS) Agreement, Covered under TRIPS Agreement, Features of the Agreement, Protection of Intellectual Property under TRIPS, Copyright and Related Rights, Trademarks, Geographical indications, Industrial Designs, Patents, Patentable Subject Matter, Rights Conferred, Exceptions, Term of protection, Conditions on Patent Applicants, Process Patents, Other Use without Authorization of the Right Holder, Layout-Designs of Integrated Circuits, Protection of Undisclosed Information, Enforcement of Intellectual Property Rights, UNSECO.

Course outcomes:

At the end of the course the student will be able to:

- Discuss research methodology and the technique of defining a research problem
- Explain the functions of the literature review in research, carrying out a literature search, developing theoretical and conceptual frameworks and writing a review.
- Explain various research designs, sampling designs, measurement and scaling techniques and also different methods of data collections.
- Explain several parametric tests of hypotheses, Chi-square test, art of interpretation and writing research reports
- Discuss various forms of the intellectual property, its relevance and business impact in the changing global business environment and leading International Instruments concerning IPR.

Question paper pattern:

- The question paper will have ten questions.
- Each full question is for 20 marks.
- There will be 2full questions (with a maximum of four sub questions in one full question) from each module.
- Each full question with sub questions will cover the contents under a module.
- Students will have to answer 5 full questions, selecting one full question from each module.

Textbooks

(1) Research Methodology: Methods and Techniques, C.R. Kothari, Gaurav Garg,New Age International,4th Edition, 2018.

(2) Research Methodology a step-by-step guide for beginners. (For the topic Reviewing the literature under module 2), RanjitKumar,SAGE Publications,3rd Edition, 2011.

(3) Study Material (For the topic Intellectual Property under module 5),
Professional Programme Intellectual Property Rights, Law and Practice, The Institute of Company Secretaries of India, Statutory Body Under an Act of Parliament, September 2013.

Reference Books

(1) Research Methods: the concise knowledge base, Trochim, Atomic Dog Publishing, 2005.

(2) Conducting Research Literature Reviews: From the Internet to Paper, Fink A, Sage Publications, 2009.

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

PRESERVING AND RECOVERING DIGITAL EVIDENCE

Course Code	**20SFC21**	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.

Module 2

Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices.

Module 3

Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet.

Module 4

Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.

Module 5

Handling the digital crime scene, digital evidence examination guidelines.

Course outcomes:
At the end of the course the student will be able to:

- Explain Digital evidence and computer crime and Laws
- Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems
- Illustrate the Networks basics for digital investigators
- Able to investigate computer intrusions and cyber stalking
- Explain the basic concepts how to handling the digital crime scene, digital evidence examination guidelines

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Digital Evidence and Computer Crime Forensic science, Computers and Internet	Eoghan Casey,	Elsevier Academic Press,	Second Edition.

Reference Books

1	Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data	Terrence V.Lillard, Glint P.Garrison, Craig A..Schiller, James Steele	Syngress	
2	The Best Damn Cybercrime and Digital Forensics Book Period'	Jack Wiles , Anthony Reyes , Jesse Varsalone	Syngress Edition	2007

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

OPERATING SYSTEM SECURITY

Course Code	**20SFC22**	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.

Module 2

Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

Module 3

Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

Module 4

Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

Module 5

Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration.
Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Course outcomes:
At the end of the course the student will be able to:

- Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.
- Analyze how to build a secure OS by exploring the early work in OS.
- Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.
- Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Shows variety of approaches applied to the development & extension services for securing operating systems.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year

1	Operating system security	Trent Jaeger	Morgan & Claypool Publishers	2008
Reference Books				
1	Guide to Operating system Security	Michael Palmer	Thomson	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC) **Choice Based Credit System (CBCS) and Outcome Based Education (OBE)** **SEMESTER - II**			
SECURED PROGRAMMING			
Course Code	**20SFC23**	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering represent able URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries. Good security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions, Trustworthy channels and trusted path, Avoiding semantics and algorithmic complexity attacks.

Module 2

Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object. Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data.

Module 3

Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa. Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision.

Module 4

Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions. Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object alignment by using realloc.

Module 5

I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files.

Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler. Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors.

Course outcomes:

At the end of the course the student will be able to:

- How to respond to security alerts which identifies software issues

- Identify possible security programming errors
- Define methodology for security testing and use appropriate tools in its implementation
- Apply new security-enhanced programming models and tools

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	The CERT ® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems	Robert C. Seacord	Addison Wesley Professional	Second Edition 2014
2	Secure Programming for Linux and Unix HowTo	David Wheeler	Linux Documentation project	2004
Reference Books				
1	Secure Programming Cookbook for C and C++	JohnViega, Matt Messier	O'Reilly Media	2003

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

CYBER LAWS AND ETHICS

Course Code	**20SFC241**	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to Cyber Law and Cyber Ethics: Introduction to Cyber Crimes and Ethical Issues in IT, Basic concepts of Law and Information Security, overview of Information Security obligations under ITA 2008, Privacy and data protection concepts.

Module 2

Law of Contracts applicable for Cyber Space transactions: introduction to Contract law, legal recognition of Electronic Documents, Authentication of Electronic Documents, Authentication of Electronic Documents, Cyber space contracts, Resolution of Contractual disputes, stamping of Contractual document.

Module 3

Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents.

Module 4

Miscellaneous Issues in Cyber Crimes and Cyber Security: Cyber Crime Investigation and Prosecution, Digital evidence and Cyber forensics, Jurisdiction issues, Information Security Management in corporate Sector..

Module 5

IT act aim and objectives, Scope of the act, Major Concepts, Important provisions, Attribution, acknowledgement, and dispatch of electronic records, Secure electronic records and secure digital signatures, Regulation of certifying authorities: Appointment of Controller and Other officers, Digital Signature certificates, Duties of Subscribers, Penalties and adjudication, The cyber regulations appellate tribunal, Offences, Network service providers not to be liable in certain cases, Miscellaneous Provisions.

Course outcomes:

At the end of the course the student will be able to:

- Describe the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
- Classify the Types of contract law, Digital signature , related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues, the types of cyber crimes and related legal issues.
- Interpret the cyber crime investigation and prosecution in depth.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Cyber Laws for Engineers	Naavi	Ujvala Consultants Pvt Ltd	2010
2.	Cryptography, Network Security and Cyber Laws	Bernard Menezes	Cengage Learning,	, 2010 edition (Chapters-25)

Reference Books

1	Computer Ethics	Deborah G Johnson	Pearson Education	
2	Ethical Decision making and Information Technology: An Introduction with Cases	Earnest A. Kallman, J.P Grillo	McGraw Hill	
3	Cyber security Operations Handbook	John W. Rittinghouse, William M. Hancock	Elsevier	
4	Michael E. Whitman, Herbert J. Mattord	Principles of Information Security	Cengage	2nd Edition
5	Network Infrastructure Security	Randy Weaver, Dawn Weaver	Cengage	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

BIOMETRIC SECURITY

Course Code	**20SFC242,** 20SAM242	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module 1

Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy inbiometric systems.

Module 2

Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics.

Module 3

Behavioural Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke
Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.

Module 4

Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Module 5

Case studies on Physiological, Behavioural and multifactor biometrics in identification systems.

Course outcomes:

At the end of the course the student will be able to:

- Visualize traditional and biometric systems.
- Analyze different algorithms of biometric systems.
- Compare strengths and weaknesses of different biometric systems.
- Design different biometric system.
- Design multimodal biometric systems.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Biometrics –Identity verification in a networked World	Samir Nanavathi, Michel Thieme, and Raj Nanavathi	Wiley Eastern	2002
2	Implementing Biometric Security	John Chirillo and Scott Blaul	Wiley Eastern Publications	2005
Reference Books				
1	Biometrics for Network Security	John Berger	Prentice Hall	2004

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

INFORMATION SECURITY POLICIES IN INDUSTRY

Course Code	**20SFC243,** 20SCN323	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.

Module 2

Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in

Organization, Business Objectives, Standards: International Standards.

Module 3

Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.

Module 4

Establishing Type of Viruses Protection: Rules for handling Third Party Software, User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key Generation considerations and Management, Software Development policies, Processes Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.

Module 5

Maintaining the Policies: Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.

Course outcomes:

At the end of the course the student will be able to:

- Explain the content, need, and responsibilities of information security policies.
- Explain the standards, guidelines, Procedures, and key roles of the organization.
- Able to write policy document for securing network connection and interfaces.
- Explain the threats to the stored data or data in transit and able to write policy document.
- Able to write, monitor, and review policy document.

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Writing Information Security Policies	Scott Barman	Sams Publishing	2002
2	Information Policies Procedures and Standards	Thomas.R.Peltier	CRC Press	2004
Reference Books				
1	Information Security Fundamentals	Thomas R Peltier, Justin Peltier, John Backley	CRC Press,	2005
2	Information Security Management Handbook	Harold F. Tipton and Micki Krause	Auerbach publications	5th Edition, 2005

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

TRUST MANAGEMENT IN E-COMMERCE

Course Code	**20SFC244,** 20SSE253	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to E-Commerce: Network and E-Commerce, Types of E-Commerce. Ecommerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models. Ecommerce Payment systems: Types of payment system, Credit card E-Commerce transactions, B2C E-Commerce Digital payment systems, B2B payment system.

Module 2

Security and Encryption: E-Commerce Security Environment, Security threats in Ecommerce environment, Policies, Procedures and Laws.

Module 3

Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of E-Commerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust, Conceptual model of inter-organizational trust in E-Commerce participation.

Module 4

Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform.

Module 5

Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain.

Course outcomes:

At the end of the course the student will be able to:

- Explain the types of E-Commerce, E-Commerce business models and E-commerce payment systems.
- Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment.
- Analysis and explain the issues, risks and challenges in inter-organisational trust in E-Commerce
- Explain the Key components and Trust mechanisms of trusted computing platform.
- Describe the Trusted platforms for organizations and individuals

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Study Guide to E-Commerce Business Technology Society	Kenneth C. Laudon and Carol GuercioTrave	Pearson Education	2005
2	Inter-Organizational Trust for Business-to-Business E-Commerce	Pauline Ratnasingam	IRM Press	2005
Reference Books				
1	Trusted Computing Platforms: TCPA Technology in Context	Siani Pearson, et al	Prentice Hall PTR	2002

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

DATA MINING & DATA WAREHOUSING

Course Code	**20SFC251**, 20SIT23, 20SSE241, 20SIS331	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction and Data Preprocessing :Why data mining, What is data mining, What kinds of data can be mined, What kinds of patterns can be mined, Which Technologies Are used, Which kinds of Applications are targeted, Major issues in data mining .Data Preprocessing: An overview, Data cleaning, Data integration, Data reduction, Data transformation and data discretization.

Module -2

Data warehousing and online analytical processing: Data warehousing: Basic concepts, Data warehouse modeling: Data cube and OLAP, Data warehouse design and usage, Data warehouse implementation, Data generalization by attribute-oriented induction,

Module – 3

Classification: Basic Concepts: Basic Concepts, Decision tree induction, Bays Classification Methods, Rule-Based classification, Model evaluation and selection, Techniques to improve classification accuracy

Module-4

Cluster Analysis: Basic concepts and methods: Cluster Analysis, Partitioning methods, Hierarchical Methods, Density-based methods, Grid-Based Methods, Evaluation of clustering.

Module-5

Data mining trends and research frontiers: Mining complex data types, other methodologies of data mining, Data mining applications, Data Mining and society.

Course outcomes:

At the end of the course the student will be able to:

- Demonstrate Storing voluminous data for online processing, Preprocess the data for mining applications
- Apply the association rules for mining the data
- Design and deploy appropriate classification techniques
- Cluster the high dimensional data for better organization of the data
- Discover the knowledge imbibed in the high dimensional system

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Data Mining Concepts and Techniques	Jiawei Han, MichelineKamber, Jian Pei	ELSEVIER	3rd edition 2012
Reference Books				
1	Data Warehousing and data mining OLAP	Alex and Stephen I smith		

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

DATABASE SECURITY

Course Code	**20SFC252,** 20SSE333, 20SCE332, 20SIT332	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take-Grant Model, Acten Model, PN Model,

Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.

Module 2

Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria.

Module 3

Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design.

Module 4

Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery.

Module 5

Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.

Course outcomes:

At the end of the course the student will be able to:

- Carry out a risk analysis for a large database
- Implement identification and authentication procedures, fine-grained access control and data encryption techniques
- Set up accounts with privileges and roles
- Audit accounts and the database system

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Database Security and Auditing	Hassan A. Afyoun	CENGAGE Learning	2009
2	Database Security	Castano	Pearson Education	
Reference Books				
1	Database security	Alfred Basta, Melissa Zgola	CENGAGE learning	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - II

ENTERPRISE APPLICATION PROGRAMMING

Course Code	**20SFC253,** 20SIT12, 20SSE22	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Web application and java EE 6: Exploring the HTTP Protocol, Introducing web applications,

describing web containers, exploring web architecture models, exploring the MVC architecture. **Working with servlets 3.0** Exploring the features of java servlet, Exploring new features in servlet 3.0, Exploring the servlet API, explaining the servlet life cycle, creating a sample servlet, creating a servlet by using annotation, working with servlet config and servlet context objects, working with the HTTP servlet request and HTTP servlet response interfaces, Exploring request delegation and request scope, implementing servlet collaboration.

Module 2

Handling sessions in servlet 3.0: Describing a session, introducing session tracking, Exploring the session tracking, mechanisms, using the java servlet API for session tracking, creating login application using session tracking. **Implementing event handling** Introducing events, Introducing event handling, working with the servlet events, developing the online shop web application. **Working with java server pages:** Introducing JSP technology, Exploring new features of JSP2.1, listing advantages of JSP over java servlet, Exploring the architecture of a JSP page, Describing the life cycle of a JSP page, working with JSP basic tags and implicit objects, working with the action tags in JSP, exploring the JSP unified EL, using functions with EL.

Module 3

Implementing JSP tag extensions: Exploring the elements of tag extensions, Working with classic tag handlers, Exploring the tag extensions, Working with simple tag handlers. **Implementing java server pages standard tag library 1.2:** Introducing JSTL, Exploring the tag libraries JSTL, working with the core tag library. **Implementing filters:** Exploring the need of filters, exploring the working of filters, exploring filters API, configuring a filter, creating a web application using filters, using initializing parameter in filters.

Module 4

Persistence Management and Design Patterns: Implementing java persistence using hibernate Introducing hibernate, exploring the architecture of hibernate, downloading hibernate, exploring HQL, understanding hibernate O/R mapping, working with hibernate,Implementing O/R mapping with hibernate. **Java EE design patterns:** Describing the java EE application architecture, Introducing a design patterns, discussing the role of design patterns, exploring types of patterns.

Module 5

Web Frameworks: Working with struts 2 Introducing struts 2, understanding actions in struts 2.**Working with java server faces 2.0:** Introducing JSF, Explaining the features of JSF, Exploring the JSF architecture, describing JSF elements, Exploring the JSF request processing life cycle. **Working with spring 3.0:** Introducing features of the spring framework, exploring the spring framework architecture, exploring dependency injection & inversion of control, exploring AOP with spring, managing transactions. **Securing java EE 6 applications:** Introducing security in java EE 6, exploring security mechanisms, implementing security on an application server.

Course outcomes:

At the end of the course the student will be able to:

- Explain WEB basics and their functionalities
- Develop JAVA support and API skills
- Build a WEB application.
- Build Security mechanisms

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	JAVA SERVER PROGRAMMING JAVA	Kogent learning solution	Dreamtech press	2014

	EE6(J2EE 1.6),			
Reference Books				
1.	Java the complete Reference	Herbert Schildt	Mc Graw Hill	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC) **Choice Based Credit System (CBCS) and Outcome Based Education (OBE)** **SEMESTER - II**			
MACHINE LEARNING TECHNIQUES			
Course Code	**20SFC254,** 20SSE334, 20LNI322, 20SCE321, 20SCN324, 20SIT322, 20SAM21	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

INTRODUCTION, CONCEPT LEARNING AND DECISION TREES
Learning Problems – Designing Learning systems, Perspectives and Issues – Concept Learning – Version Spaces and Candidate Elimination Algorithm – Inductive bias – Decision Tree learning – Representation – Algorithm – Heuristic Space Search

Module -2

NEURAL NETWORKS AND GENETIC ALGORITHMS: Neural Network Representation – Problems – Perceptrons – Multilayer Networks and Back Propagation Algorithms – Advanced Topics – Genetic Algorithms – Hypothesis Space Search – Genetic Programming – Models of Evolution and Learning.

Module – 3

BAYESIAN AND COMPUTATIONAL LEARNINGL Bayes Theorem – Concept Learning – Maximum Likelihood – Minimum Description Length Principle – Bayes Optimal Classifier – Gibbs Algorithm – Naïve Bayes Classifier– Bayesian Belief Network – EM Algorithm – Probably Learning – Sample Complexity for Finite and Infinite Hypothesis Spaces – Mistake Bound Model.

Module-4

INSTANT BASED LEARNING AND LEARNING SET OF RULES: K- Nearest Neighbor Learning – Locally Weighted Regression – Radial Basis Functions –Case-Based Reasoning – Sequential Covering Algorithms – Learning Rule Sets – Learning First Order Rules – Learning Sets of First Order Rules – Induction as Inverted Deduction – Inverting Resolution

Module-5

ANALYTICAL LEARNING AND REINFORCED LEARNING: Perfect Domain Theories – Explanation Based Learning – Inductive-Analytical Approaches - FOCL Algorithm – Reinforcement Learning – Task – Q-Learning – Temporal Difference Learning

Course outcomes:
At the end of the course the student will be able to:

- Choose the learning techniques with this basic knowledge.
- Apply effectively neural networks and genetic algorithms for appropriate applications.
- Apply bayesian techniques and derive effectively learning rules.
- Choose and differentiate reinforcement and analytical learning techniques
-

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year

1	Machine Learning	Tom M. Mitchell	McGraw-Hill Education	2013
Reference Books				
1	Introduction to Machine Learning	EthemAlpaydin	PHI Learning Pvt. Ltd	2nd Ed., 2013
2	The Elements of Statistical Learning	T. Hastie, R. Tibshirani, J. H. Friedman	Springer	1st edition, 2001

TECHNICAL SEMINAR			
Course Code	20SFC27	CIE Marks	100
Number of contact Hours/week (L:P:SDA)	0:0:2	SEE Marks	--
Credits	02	Exam Hours	--

Course objectives:

The objective of the seminar is to inculcate self-learning, face audience confidently, enhance communication skill, involve in group discussion and present and exchange ideas.

Each student, under the guidance of a Faculty, is required to

- Choose, preferably through peer reviewed journals, a recent topic of his/her interest relevant to the Course of Specialization.
- Carryout literature survey, organize the Course topics in a systematic order.
- Prepare the report with own sentences.
- Type the matter to acquaint with the use of Micro-soft equation and drawing tools or any such facilities.
- Present the seminar topic orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit two copies of the typed report with a list of references.

The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

The CIE marks for the seminar shall be awarded (based on the relevance of the topic, presentation skill, participation in the question and answer session and quality of report) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculties from the department with the senior most acting as the Chairperson.

Marks distribution for CIE of the course 20XXX27 seminar:

Seminar Report: 30 marks

Presentation skill:50 marks

Question and Answer:20 marks

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

FILE SYSTEM FORENSIC ANALYSIS

Course Code	**20SFC31**, 20SCS323	CIE Marks	40
Teaching Hours/Week (L:P:S)	3:0:2	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions, Multiple Disk Volumes: RAID, Disk Spanning.

Module 2

File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture, Other Topics. FAT Data Structures: Boot Sector, FAT32 FSINFO, FAT, Directory Entries, Long File Name Directory Entries

Module 3

NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools.
NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture.
NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures, File System Metadata Files.

Module 4

Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture.
Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes, Directory Entry, Symbolic Link, Hash Trees, Journal Data Structures

Module 5

UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture.
UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor, Block and Fragment Bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended Attributes, Directory Entries

Course outcomes:
At the end of the course the student will be able to:

- Compare the different file systems for storing information
- Illustrate the role of computer forensics in the business and private world
- Identify some of the current techniques and tools for forensic examinations

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.

- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	File System Forensic Analysis	Brian Carrier	Pearson Education	2005
Reference Books				
1	Introduction to Linux A Hands-On Guide	MachteltGarrels	Fultus Corporation Publisher	Third Edition2010

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

SECURITY ARCHITECTURE DESIGN

Course Code	**20SFC321**	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Architecture and Security: Architecture Reviews, Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments, Security Architecture Basics, Architecture Patterns in Security

Module 2

Low-Level Architecture: Code Review, importance of code review, Buffer Overflow Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications.

Module 3

Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility, The Common Object Request Broker Architecture, The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security.

Module 4

High-Level Architecture: Security Components, Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment,The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability.

Module 5

Enterprise Security Architecture: Security as a Process, Security Data, Enterprise Security as a Data Management Problem, Tools for Data Management, David Isenberg and the "Stupid Network", Extensible MarkupLanguage,The XML Security Services Signaling Layer, XML and Security Standards, The Security Pattern Catalog Revisited, XML-Enabled Security Data-HGP: A Case Study in Data Management, Business Cases and Security, Building Business Cases for Security **Case study:** Building secure OS for Linux: Linux security modules, security enhanced Linux.

Course outcomes:
At the end of the course the student will be able to:

- Design the secured sites based on tools & techniques
- Map site zones with level of security
- Identify the components targeted for each zone

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to

60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Designing Security Architecture Solutions	Jay Ramachandran	Wiley Computer Publishing	2010.
Reference Books				
1	Security Patterns: Integrating Security and Systems Engineering	Markus Schumacher	Wiley Software Pattern Series	2010

M.TECH COMPUTER SCIENCE AND ENGINEERING (SCS)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER -III

STEGANOGRAPHY AND DIGITAL WATERMARKING

Course Code	**20SFC322**	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to Information hiding: Brief history and applications of information hiding, Principles of Steganography, Frameworks for secret communication, Security of Steganography systems, Information hiding in noisy data, Adaptive versus non adaptive algorithms, Laplace filtering, Using cover models, Active and malicious attackers, Information hiding in written text, Examples of invisible communications.

Module-2

Survey of steganographic techniques: Substitution system and bit plane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.

Module-3

Steganalysis: Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system.

Module-4

Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace, binary image, audio, video. Formatting the watermark beds: Digital watermarking schemes, Spread Spectrum, DCT (Discrete Cosine Transform), Domain and Quantization schemes, Watermarking with side information, Robustness to temporal and geometric distortions.

Module-5

Data Right Management: DRM Products and Laws, Fingerprints, Examples, Protocols and Codes, Boneh-Shaw finger printing Scheme, Steganography and watermarking applications, Military, Digital copyright protection and protection of intellectual property.

Course outcomes:

At the end of the course the student will be able to:

- Distinguish Stegnography& Digital watermarking from other related fields.
- Knowledge of how to use steganography techniques in conjunction with encryption systems to protect data.

- Explain different types of watermarking applications and watermarking frameworks.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Information hiding techniques for Steganography and Digital Watermarking	Stefan Katzenbelsser and Fabien A. P. Petitcolas	ARTECH House	January 2004
	Digital Water Marking and Steganography	I.J. Cox, M.L. Miller, J.Fridrich and T.Kalker	Morgan Kauffman	2nd Edition 2008
	Information Hiding: Steganography and Watermarking -Attacks and Countermeasures	Johnson, Neil F. / Duric, Zoran / Jajodia, Sushil G	Advances in Information Security	2001
Reference Books				
1	Disappearing Cryptography: Information Hiding, Steganography and Watermarking	Peter Wayner	Elsevier	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

MOBILE DEVICE FORENSICS

Course Code	**20SFC323**	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics

Module 2

Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices

Module 3

Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.

Module 4

Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques

Module 5

Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis

Course outcomes:
At the end of the course the student will be able to:

- Describe security risks and vulnerabilities from mobile devices and network access.
- Explain the methods and procedures used in forensics investigations.
- Have knowledge of the global security threats and vulnerabilities of mobile devices and networks.
- Carry out a forensics investigation of mobile and network devices.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Android Forensics Investigation, Analysis, and Mobile security for Google Android	Andrew Hoog, John McCash, , Technical Editor	Elsevier,	2011
Reference Books				
1	Practical Mobile Forensics	SatishBommisetty, RohitTamma, Heather Mahalik	Packt Publishing	2014
2	Mobile Device Forensics	Andrew Martin	SANS Institute	2009

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

SECURITY ASSESSMENT AND VERIFICATION

Course Code	**20SFC324**	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Module 2

Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information.

Module 3

Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Module 4

Security Risk assessment project management, Security risk assessment approaches and methods.

Module 5

Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.

Course outcomes:
At the end of the course the student will be able to:

- Illustrate the roles information security and its management
- Select appropriate techniques to tackle and solve problems in the discipline of information security assessment
- Design an information security and validation system

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	A practical guide to security assessments	SudhanshuKairab	CRC press	2005
2	A Security risk assessment Handbook	Douglas J. Landoll	Auerbach publications	2006
Reference Books				
1	Principles of Information Security	Michael E. Whitman, Herbert J. Mattord	Cengage Learning	2nd Edition
2	Information Security Fundamentals	Thomas R Peltier, Justin Peltier and John Blackley	Prentice Hall	2nd Edition, 1996

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

MANAGING BIG DATA

Course Code	**20SFC331**, 20SIT31, 20LNI251, 20SCE21, 20SIS332	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Meet Hadoop: Data!, Data Storage and Analysis, Querying All Your Data, Beyond Batch, Comparison with Other Systems: Relational Database Management Systems, Grid Computing, Volunteer Computing Hadoop Fundamentals MapReduce A Weather Dataset: Data Format, Analyzing the Data with Unix Tools, Analyzing the Data with Hadoop: Map and Reduce, Java MapReduce, Scaling Out: Data Flow, Combiner Functions, Running a Distributed MapReduce Job, Hadoop Streaming

The Hadoop Distributed Filesystem The Design of HDFS, HDFS Concepts: Blocks, Namenodes and Datanodes, HDFS Federation, HDFS High-Availability, The Command-Line Interface, Basic Filesystem Operations, HadoopFilesystems Interfaces, The Java Interface, Reading Data from a Hadoop URL, Reading Data Using the FileSystem API, Writing Data, Directories, Querying the Filesystem, Deleting Data, Data Flow: Anatomy of a File Read, Anatomy of a File Write.

Module -2

YARN Anatomy of a YARN Application Run: Resource Requests, Application Lifespan, Building YARN Applications, YARN Compared to MapReduce, Scheduling in YARN: The FIFO Scheduler, The Capacity Scheduler, The Fair Scheduler, Delay Scheduling, Dominant Resource Fairness

Hadoop I/O Data Integrity, Data Integrity in HDFS, LocalFileSystem, ChecksumFileSystem, Compression, Codecs, Compression and Input Splits, Using Compression in MapReduce, Serialization, The Writable Interface, Writable Classes, Implementing a Custom Writable, Serialization Frameworks, File-Based Data Structures: SequenceFile

Module – 3

Developing a MapReduce Application The Configuration API, Combining Resources, Variable Expansion, Setting Up the Development Environment, Managing Configuration, GenericOptionsParser, Tool, and ToolRunner, Writing a Unit Test with MRUnit: Mapper, Reducer, Running Locally on Test Data, Running a Job in a Local Job Runner, Testing the Driver, Running on a Cluster, Packaging a Job,

Launching a Job, The MapReduce Web UI, Retrieving the Results, Debugging a Job, Hadoop Logs, Tuning a Job, Profiling Tasks, MapReduce Workflows: Decomposing a Problem into MapReduce Jobs, JobControl, Apache Oozie

How MapReduce Works Anatomy of a MapReduce Job Run, Job Submission, Job Initialization, Task Assignment, Task Execution, Progress and Status Updates, Job Completion, Failures: Task Failure, Application Master Failure, Node Manager Failure, Resource Manager Failure, Shuffle and Sort: The Map Side, The Reduce Side, Configuration Tuning, Task Execution: The Task Execution Environment, Speculative Execution, Output Committers

Module-4

MapReduce Types and Formats: MapReduce Types, Input Formats: Input Splits and Record,s Text Input, Binary Input, Multiple Inputs, Database Input (and Output) Output Formats: Text Output, Binary Output, Multiple Outputs, Lazy Output, Database Output,

Flume Installing Flume, An Example,Transactions and Reliability, Batching, The HDFS Sink, Partitioning and Interceptors, File Formats, Fan Out, Delivery Guarantees, Replicating and Multiplexing Selectors, Distribution: Agent Tiers, Delivery Guarantees, Sink Groups, Integrating Flume with Applications, Component Catalog

Module-5

Pig Installing and Running Pig, Execution Types, Running Pig Programs, Grunt, Pig Latin Editors, An Example: Generating Examples, Comparison with Databases, Pig Latin: Structure, Statements, Expressions, Types, Schemas, Functions, Data Processing Operators: Loading and Storing Data, Filtering Data, Grouping and Joining Data, Sorting Data, Combining and Splitting Data.

Spark An Example: Spark Applications, Jobs, Stages and Tasks, A Java Example, A Python Example, Resilient Distributed Datasets: Creation, Transformations and Actions, Persistence, Serialization, Shared Variables, Broadcast Variables, Accumulators, Anatomy of a Spark Job Run, Job Submission, DAG Construction, Task Scheduling, Task Execution, Executors and Cluster Managers: Spark on YARN

Course outcomes:

At the end of the course the student will be able to:

- Understand managing big data using Hadoop and SPARK technologies
- Explain HDFS and MapReduce concepts
- Install, configure, and run Hadoop and HDFS.
- Perform map-reduce analytics using Hadoop and related tools
- Explain SPARK concepts

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Hadoop: The Definitive Guide	Tom White	O'Reilley	Third Edition, 2012
Reference Books				
1	SPARK: The Definitive Guide	MateiZaharia and Bill Chambers	Oreilly	2018
2	Apache Flume: Distributed Log Collection for Hadoop	. D'Souza and Steve Hoffman	Oreilly	2014

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

MOBILE APPLICATION DEVELOPMENT

Course Code	**20SFC332,** 20LNI323, 20SCN244, 20SIT241,	CIE Marks	40

	20SIS252		
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to mobile communication and computing: Introduction to mobile computing, Novel applications, limitations and GSM architecture, Mobile services, System architecture, Radio interface, protocols, Handover and security. Smart phone operating systems and smart phones applications.

Module -2

Fundamentals of Android Development: Introduction to Android., The Android 4.1 Jelly Bean SDK, Understanding the Android Software Stack, Installing the Android SDK, Creating Android Virtual Devices, Creating the First Android Project, Using the Text View Control, Using the Android Emulator.

Module – 3

The Intent of Android Development, Four kinds of Android Components: Activity, Service, Broadcast Receiver and Content Provider. Building Blocks for Android Application Design, Laying Out Controls in Containers. Graphics and Animation: Drawing graphics in Android, Creating Animation with Android's Graphics API.

Module-4

Creating the Activity, Working with views: Exploring common views, using a list view, creating custom views, understanding layout. Using Selection Widgets and Debugging Displaying and Fetching Information Using Dialogs and Fragments. Multimedia: Playing Audio, Playing Video and Capturing Media. Advanced Android Programming: Internet, Entertainment, and Services.

Module-5

Displaying web pages and maps, communicating with SMS and emails. Creating and using content providers: Creating and consuming services, publishing android applications

Course outcomes:

At the end of the course the student will be able to:

- Describe the requirements for mobile applications
- Explain the challenges in mobile application design and development
- Develop design for mobile applications for specific requirements
- Implement the design using Android SDK
- Implement the design using Objective C and iOS
- Deploy mobile applications in Android and iPone marketplace for distribution

Question paper pattern:

The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Mobile Computing: (technologies and Applications	N. N. Jani	S chand	
2	Android programming	B.M.Hirwani	Pearson publications	2013
3	Android in Action	W. Frank Ableson, RobiSen and C. E. Ortiz	DreamTech Publisher	Third Edition-2012

Reference Books

1.	Android application development	James C.Sheusi	Cengage	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

SOCIAL NETWORK ANALYSIS

Course Code	**20SFC333**, 20LNI332, 20SCN252	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

Introduction to social network analysis and Descriptive network analysis: Introduction to new science of networks. Networks examples. Graph theory basics. Statistical network properties. Degree distribution, clustering coefficient. Frequent patterns. Network motifs. Cliques and k-cores.

Module 2

Network structure, Node centralities and ranking on network: Nodes and edges, network diameter and average path length. Node centrality metrics: degree, closeness and betweenness centrality. Eigenvector centrality and PageRank. Algorithm HITS.

Module 3

Network communities and Affiliation networks: Networks communities. Graph partitioning and cut metrics. Edge betweenness. Modularity clustering. Affiliation network and bipartite graphs. 1-mode projections. Recommendation systems.

Module 4

Information and influence propagation on networks and Network visualization: Social Diffusion. Basic cascade model. Influence maximization. Most influential nodes in network. Network visualization and graph layouts. Graph sampling. Low -dimensional projections

Module 5

Social media mining and SNA in real world: FB/VK and Twitter analysis: Natural language processing and sentiment mining. Properties of large social networks: friends, connections, likes, re-tweets.

Course outcomes:
At the end of the course the student will be able to:

- Define notation and terminology used in network science.
- Demonstrate, summarize and compare networks.
- Explain basic principles behind network analysis algorithms.
- Analyzing real world network.

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.
- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Networks, Crowds, and Markets: Reasoning About a Highly Connected World	David Easley and John Kleinberg	Cambridge University Press	2010
2	Statistical Analysis of Network Data with R	Eric Kolaczyk, Gabor Csardi	Springer	2014
3	Social Network Analysis. Methods and Applications	Stanley Wasserman and Katherine Faust	Cambridge University Press	1994
Reference Books				
1.	Statistical Analysis of Network Data with R	Gabor Csardi	Springer	

M.TECH IN CYBER FORENSICS AND INFORMATION SECURITY (SFC)
Choice Based Credit System (CBCS) and Outcome Based Education (OBE)
SEMESTER - III

SOFTWARE METRICS & QUALITY ASSURANCE

Course Code	**20SFC334**, 20SIT243, 20SSE242	CIE Marks	40
Teaching Hours/Week (L:P:S)	4:0:0	SEE Marks	60
Credits	04	Exam Hours	03

Module-1

What Is Software Quality: Quality: Popular Views, Quality Professional Views, Software Quality, Total Quality Management and Summary. **Fundamentals Of Measurement Theory:** Definition, Operational Definition, And Measurement, Level Of Measurement, Some Basic Measures, Reliability And Validity, Measurement Errors, Be Careful With Correlation, Criteria For Causality, Summary. **Software Quality Metrics Overview:** Product Quality Metrics, In Process Quality Metrics, Metrics for Software Maintenance, Examples For Metrics Programs, Collecting Software Engineering Data.

Module -2

Applying The Seven Basic Quality Tools In Software Development: Ishikawa's Seven Basic Tools, Checklist, Pareo Diagram, Histogram, Run Charts, Scatter Diagram, Control Chart, Cause And Effect Diagram. **The Rayleigh Model:** Reliability Models, The Rayleigh Model Basic Assumptions, Implementation, Reliability And Predictive Validity.

Module – 3

Complexity Metrics And Models: Lines Of Code, Halstead's Software Science ,Cyclomatic Complexity Syntactic Metrics, An Example Of Module Design Metrics In Practice .**Metric And Lessons Learned For Object Oriented Projects:** Object Oriented Concepts And Constructs, Design And Complexity Metrics, Productivity Metrics, Quality And Quality Management Metrics, Lessons Learned For object oriented Projects.

Module-4

Availability Metrics: Definition And Measurement Of System Availability, Reliability Availability And Defect Rate, Collecting Customer Outage Data For Quality Improvement, In Process Metrics For Outage And Availability .**Conducting Software Project Assessment :**Audit Ad Assessment , Software Process Maturity Assessment And Software Project Assessment , Software Process Assessment A Preponed Software Project Assessment Method.

Module-5

Dos And Don'ts Of Software Process Improvement : Measuring Process Maturity, Measuring Process Capability, Staged Versus Continuous Debating Religion, Measuring Levels Is Not Enough, Establishing The Alignment Principle , Take Time Getting Faster, Keep it Simple Or Face Decomplexification, Measuring The Value Of Process Improvement , Measuring Process Compliance , Celebrate The Journey Not Just The Destination. **Using Function Point Metrics to Measure Software Process Improvement: Software** Process Improvement Sequences, Process Improvement Economies, Measuring Process Improvement at Activity Levels

Course outcomes:
At the end of the course the student will be able to:

- Identify and apply various software metrics, which determines the quality level of software
- Identify and evaluate the quality level of internal and external attributes of the software product
- Compare and Pick out the right reliability model for evaluating the software
- Evaluate the reliability of any given software product
- Design new metrics and reliability models for evaluating the quality level of the software based on the requirement

Question paper pattern:
The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 60.

- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks.

- There will be two full questions (with a maximum of four sub questions) from each module.
- Each full question will have sub question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module.

Textbook/ Textbooks

Sl No	Title of the book	Name of the Author/s	Publisher Name	Edition and year
1	Metrics and Models in Software Quality Engineering,	Stephen H Khan	Pearson	2nd edition 2013
Reference Books				
1	Software Metrics	Norman E-Fentor and Share Lawrence Pflieger	International Thomson Computer Press	1997
2	Software quality and Testing Market,.	S.A.Kelkar	PHI Learning, Pvt, Ltd	2012
3	Managing the Software Inc,.	Watts S Humphrey	Process Pearson Education	2008
4	CMMI	Mary Beth Chrissis, Mike Konrad and Sandy	Pearson Education(Singapore	2003
5	Quality is Free: The Art of Making Quality Certain	Philip B Crosby	Mass Market	1992

PROJECT WORK PHASE – 1			
Course Code	20SFC34	CIE Marks	100
Number of contact Hours/Week	2	SEE Marks	--
Credits	02	Exam Hours	--

Course objectives:

- Support independent learning.
- Guide to select and utilize adequate information from varied resources maintaining ethics.
- Guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- Develop interactive, communication, organisation, time management, and presentation skills.
- Impart flexibility and adaptability.
- Inspire independent and team working.
- Expand intellectual capacity, credibility, judgement, intuition.
- Adhere to punctuality, setting and meeting deadlines.
- Instil responsibilities to oneself and others.
- Train students to present the topic of project work in a seminar without any fear, face audience confidently, enhance communication skill, involve in group discussion to present and exchange ideas.

Project Phase-1 Students in consultation with the guide/s shall carry out literature survey/ visit industries to finalize the topic of the Project. Subsequently, the students shall collect the material required for the selected project, prepare synopsis and narrate the methodology to carry out the project work.

Seminar: Each student, under the guidance of a Faculty, is required to

- Present the seminar on the selected project orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit two copies of the typed report with a list of references.

The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Course outcomes:

At the end of the course the student will be able to:

- Demonstrate a sound technical knowledge of their selected project topic.
- Undertake problem identification, formulation, and solution.
- Design engineering solutions to complex problems utilising a systems approach.
- Communicate with engineers and the community at large in written an oral forms.
- Demonstrate the knowledge, skills and attitudes of a professional engineer.

Continuous Internal Evaluation

CIE marks for the project report (50 marks), seminar (30 marks) and question and answer (20 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session by the student) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

MINI PROJECT			
Course Code	20SFC35	CIE Marks	40
Number of contact Hours/Week	2	SEE Marks	60
Credits	02	Exam Hours/Batch	03

Course objectives:

- To support independent learning and innovative attitude.
- To guide to select and utilize adequate information from varied resources upholding ethics.
- To guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- To develop interactive, communication, organisation, time management, and presentation skills.
- To impart flexibility and adaptability.
- To inspire independent and team working.
- To expand intellectual capacity, credibility, judgement, intuition.
- To adhere to punctuality, setting and meeting deadlines.
- To instil responsibilities to oneself and others.
- To train students to present the topic of project work in a seminar without any fear, face audience confidently, enhance communication skill, involve in group discussion to present and exchange ideas.

Mini-Project: Each student of the project batch shall involve in carrying out the project work jointly in constant consultation with internal guide, co-guide, and external guide and prepare the project report as per the norms avoiding plagiarism.

Course outcomes:

At the end of the course the student will be able to:

- Present the mini-project and be able to defend it.
- Make links across different areas of knowledge and to generate, develop and evaluate ideas and information so as to apply these skills to the project task.
- Habituated to critical thinking and use problem solving skills.
- Communicate effectively and to present ideas clearly and coherently in both the written and oral forms.
- Work in a team to achieve common goal.
- Learn on their own, reflect on their learning and take appropriate actions to improve it.

CIE procedure for Mini - Project:

The CIE marks awarded for Mini - Project, shall be based on the evaluation of Mini - Project Report, Project Presentation skill and Question and Answer session in the ratio 50:25:25.The marks awarded for Mini - Project report shall be the same for all the batch mates.

Semester End Examination

SEE marks for the mini-project shall be awarded based on the evaluation of Mini-Project Report, Presentation skill and Question and Answer session in the ratio 50:25:25 by the examiners appointed by the University.

INTERNSHIP / PROFESSIONAL PRACTICE			
Course Code	20SFCI36	CIE Marks	40
Number of contact Hours/Week	2	SEE Marks	60
Credits	06	Exam Hours	03

Course objectives:

Internship/Professional practice provide students the opportunity of hands-on experience that include personal training, time and stress management, interactive skills, presentations, budgeting, marketing, liability and risk management, paperwork, equipment ordering, maintenance, responding to emergencies etc. The objective are further,

To put theory into practice.

To expand thinking and broaden the knowledge and skills acquired through course work in the field.

To relate to, interact with, and learn from current professionals in the field.

To gain a greater understanding of the duties and responsibilities of a professional.

To understand and adhere to professional standards in the field.

To gain insight to professional communication including meetings, memos, reading, writing, public speaking, research, client interaction, input of ideas, and confidentiality.

To identify personal strengths and weaknesses.

To develop the initiative and motivation to be a self-starter and work independently.

Internship/Professional practice: Students under the guidance of internal guide/s and external guide shall take part in all the activities regularly to acquire as much knowledge as possible without causing any inconvenience at the place of internship.

Seminar: Each student, is required to

- Present the seminar on the internship orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit the report duly certified by the external guide.
- The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Course outcomes:

At the end of the course the student will be able to:

- Gain practical experience within industry in which the internship is done.
- Acquire knowledge of the industry in which the internship is done.
- Apply knowledge and skills learned to classroom work.
- Develop a greater understanding about career options while more clearly defining personal career goals.
- Experience the activities and functions of professionals.
- Develop and refine oral and written communication skills.
- Identify areas for future knowledge and skill development.
- Expand intellectual capacity, credibility, judgment, intuition.
- Acquire the knowledge of administration, marketing, finance and economics.

Continuous Internal Evaluation

CIE marks for the Internship/Professional practice report (20 marks), seminar (10 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session by the student) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Semester End Examination

SEE marks for the internship report (30 marks), seminar (20 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session) by the examiners appointed by the University.

PROJECT WORK PHASE -2			
Course Code	20SFC41	CIE Marks	40
Number of contact Hours/Week	4	SEE Marks	60
Credits	20	Exam Hours	03

Course objectives:

- To support independent learning.
- To guide to select and utilize adequate information from varied resources maintaining ethics.
- To guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- To develop interactive, communication, organisation, time management, and presentation skills.
- To impart flexibility and adaptability.
- To inspire independent and team working.
- To expand intellectual capacity, credibility, judgement, intuition.
- To adhere to punctuality, setting and meeting deadlines.
- To instil responsibilities to oneself and others.
- To train students to present the topic of project work in a seminar without any fear, face audience confidently, enhance communication skill, involve in group discussion to present and exchange ideas.

Project Work Phase - II: Each student of the project batch shall involve in carrying out the project work jointly in constant consultation with internal guide, co-guide, and external guide and prepare the project report as per the norms avoiding plagiarism.

Course outcomes:

At the end of the course the student will be able to:

- Present the project and be able to defend it.
- Make links across different areas of knowledge and to generate, develop and evaluate ideas and information so as to apply these skills to the project task.
- Habituated to critical thinking and use problem solving skills
- Communicate effectively and to present ideas clearly and coherently in both the written and oral forms.
- Work in a team to achieve common goal.
- Learn on their own, reflect on their learning and take appropriate actions to improve it.

Continuous Internal Evaluation:

Project Report: 20 marks. The basis for awarding the marks shall be the involvement of the student in the project and in the preparation of project report. To be awarded by the internal guide in consultation with external guide if any.

Project Presentation: 10 marks.

The Project Presentation marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Question and Answer: 10 marks.

The student shall be evaluated based on the ability in the Question and Answer session for 10 marks.

Semester End Examination

SEE marks for the project report (30 marks), seminar (20 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session) by the examiners appointed by the University.