BHARATHIAR UNIVERSITY: COIMBATORE 641 046

M.Sc – INFORMATION SECURITY AND DIGITAL FORENSICS (2 YEARS)
(For the CCII students admitted during the academic year 2016 -2017)

1. Eligibility for Admission to the Programme

Candidates for admission to the first year programme leading to the Degree of Master of Science in Information Security and Digital Forensics (M.Sc IS& DF) will be required to possess: A Pass with 50% of marks in B.Sc - Computer Science/ Physics/ Mathematics/ Electronics , Statistics/ Information Systems/ Computer Technology/ Information Technology/ Forensic Science/ Information Security/ Cyber Forensics/ Digital Forensics/ B.Tech/ B. E - Computer Science Engineering, EEE, EIE, ME, Information Security, B.C.A./ B.Com Computer Application/ any U.G degree with minimum three years of experience in IT industry / Internationally recognized Networking certification. In case of SC/ST candidates, a mere pass in any of the above Bachelor's degree will be sufficient.

2. Duration of the Programme

The programme shall be offered on a full-time basis. The programme will consist of three semesters of course work and laboratory work and the fourth semester consists of project work.

3. Regulations

The general Regulations of the Bharathiar University Choice Based Credit System Programme are applicable to this programme.

4. The Medium of Instruction and Examinations

The medium of instruction and Examinations shall be in English.

5. Submission of Record Notebooks for Practical Examinations & Project Viva-Voce

Candidates taking the Practical Examinations should submit bonafide Record Note Books prescribed for the Examinations. Otherwise the candidates will not be permitted to take the Practical Examinations.

Candidates taking the Project Viva Examination should submit Project Report prescribed for the Examinations. Otherwise the candidates will not be permitted to take the Project Viva-voce Examination.

6. Ranking

A candidate who qualifies for the PG Degree Course passing all the Examinations in the first attempt, within the minimum period prescribed for the Course of Study from the date of admission to the Course and secures 1st or 2nd Class shall be eligible for ranking and such ranking will be confined to 10% of the total number of candidates qualified in that particular subject to a maximum of 10 ranks.

7. Revision of Regulations and Curriculum

The above Regulation and Scheme of Examinations will be in vogue without any change for a minimum period of three years from the date of approval of the Regulations. The University may revise /amend/ change the Regulations and Scheme of Examinations, if found necessary.

BHARATHIAR UNIVERSITY: COIMBATORE 641 046
M.Sc – INFORMATION SECURITY AND DIGITAL FORENSICS (2 YEARS)
(For the CCII students admitted during the academic year 2016 -2017)

SCHEME OF EXAMINATION – CBCS PATTERN

Core/ Elective/ Practical Project	Suggested Code	Semester	Title of the Paper	L	P	Credits	EXAMINATION			
							Hours	Internals	Externals	Marks
Core 1		I	Information Security	4	0	4	4	25	75	100
Core 2			Digital Forensics	4	0	4	4	25	75	100
Core 3			Computer Networks	4	0	4	4	25	75	100
Core 4			Cyber Crime	4	0	4	4	25	75	100
Elective 1			Elective-I	4	0	4	4	25	75	100
Practical 1			Digital Forensics – Lab I	0	4	4	8	40	60	100
Practical 2			Computer Networks Lab	0	4	4	8	40	60	100
Core 5		II	Network Security	4	0	4	4	25	75	100
Core 6			Advanced Information Security	4	0	4	4	25	75	100
Core 7			Digital Forensics Tools	4	0	4	4	25	75	100
Core 8			Threats in Social Media	4	0	4	4	25	75	100
Elective 2			Elective-II	4	0	4	4	25	75	100
Practical 3			Digital Forensics - Lab II	0	4	4	8	40	60	100
Practical 4			Network Security Lab	0	4	4	8	40	60	100
Core9		III	Mobile Security	4	0	4	4	25	75	100
Core 10			IT Governance, Risk and Compliance	4	0	4	4	25	75	100
Core 11			Business Continuity Planning (BCP) and Disaster Recovery (DR)	4	0	4	4	25	75	100
Core 12			Cloud Computing	4	0	4	4	25	75	100
Elective 3			Elective-III	4	0	4	4	25	75	100
Practical 5			Mobile Security Lab	0	4	4	8	40	60	100
Practical 6			Cloud Computing Lab	0	4	4	8	40	60	100
Project 1		IV	Project *	-	-	6	-	-	-	150
Total				-	-	90	-	-	-	2250

* For Project report - 80%; Viva-voce - 20%

Electives for M.Sc. IS & DF

Semester	Suggested Code	Title of the Paper	Credits
		Cyber Law	4
		Cyber Criminology	4
		Intellectual Property Rights	4
		E-mail forensics	4
		Digital Frauds	4
		Ethical Hacking	4
		Digital Preservation	4

Information Security

Subject Code: **Number of Credits: 04**

Subject Description: This course presents an overview of Information Security and its domains, classification of assets and managing the risks.

Goals: The students will be expected to understand the basic information about security management concepts, Risk management (RM) practices, and basic information on classification levels

Objective: On successful completion of the course the student should have understood the concepts of information security domains and its classification, risk management assessment tools

Contents

Unit 1: Overview of Information Security - Threats - Frauds, Thefts, Malicious Hackers, Malicious Code, Denial-of-Services Attacks and Social Engineering, Vulnerability – Types, Risk – an introduction - Business Requirements - Information Security Definitions - Security Policies – Tier-1 (Origination-Level), Tier-2 (Function Level), Tier-3 (Application/Device Level) – Procedures - Standards – Guidelines – Baselines

Unit 2: Information Asset Classification – Information system Asset inventory, Asset Classification criteria, roles and responsibilities – Methodology - Declassification or Reclassification - Retention and Disposal of Information Assets - Provide Authorization for Access.

Unit 3: Risk Management – Need for the Risk Assessment, Risk Assessment Methodology, Risk Assessment Components, Risk Mitigation Techniques.

Unit 4: Information Security – Fundamental Principles of Security – Security Definitions - Control types – Security Frameworks - Personnel Security.

Unit 5: Introduction to Security Domains – Application Security, Legal & Compliance, Business Continuity Management, Cryptography, Physical & Environmental Security and Security Operations

REFERENCES:

1. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
2. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012
3. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
4. Certified Information Systems Security Professional, Study Guide by Ed Tittel, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012
5. ISO/ IEC 27002: 2005, First Edition

Digital Forensics

Subject Code: **Number of Credits: 04**
Subject Description: Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored as data or magnetically encoded information

Goals: The students will be expected to experience in computer forensics evidence capture and analysis

Objective: On successful completion of the course the student should know how to analyze and conduct computer forensics examination.

Contents
Unit 1: Digital Forensics overview – Difference between computer Forensics and Digital Forensics, Digital Forensics in today's world, Computer Forensics investigation process, Forensics readiness planning and its benefits.

Unit 2: Understanding Digital Forensic Investigation – Digital Forensics Life Cycle **- U**nderstanding key steps in Forensics investigation, Role of forensic investigator – Ethics of a forensic investigator – challenges faced by forensic investigators.

Unit 3: Role of Digital Evidence - Digital Evidence – Authentication of Evidence - Importance of digital evidences in investigation and in court of law – Capabilities of a digital forensic investigator.

Unit 4: Computer Forensics Investigation Process - Cyber Forensics investigation methodology, steps to prepare for a computer forensics investigation, procedure to collect evidence in crime scene, search warrants, evaluate and secure the crime scene

Unit 5: Digital Evidence collection – Evidence Collection - Collections Options – Obstacles - Types of Evidence - Standards of Evidence - The rules of Evidence - Volatile Evidence– Electronic Evidence General Procedure - Collection and Archiving of evidence - Methods of Collection – Artifacts - Controlling Contamination - Chain of custody

REFERENCES:

1. Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras, 1st edition, Jones and Bartlett Publishers, 1 February 2011
2. Computer Forensics, Computer Crime Scene Investigation by John.R.Vacca, 2nd Edition, Charles River Media Publication, 15 June 2002
3. Cyber Forensics: A field manual for collecting, Examining, preserving evidence of computer crimes by Albert Marcella, Jr., Doug Menendez, Second Edition, CRC Press 2007
4. Guide to Computer Forensics and Investigations, Processing Digital Evidence by Bill Nelson, Amelia Phillips, Christopher Steuart, 4th edition, Delmar Cengage Learning, 28 Oct 2009
5. Digital Forensics for Legal Professionals - Understanding Digital Evidence from the Warrant to the Courtroom by Larry Daniel, Lars Daniel, 1st edition, Syngress, 14 October 2011

Computer Networks

Subject Code: **Number of Credits: 04**
Subject Description: The function of Network Security management includes the management of networks and security systems.

Goals: The students will be expected to understand the function and how they are relevant to security

Objective: The students should understand the following:

a. Network security transmissions in terms of local area, wide area, and remote access
b. Internet/intranet/extranet in terms of firewalls, routers, gateways, and various protocols
c. OSI model

Contents

Unit 1: Introduction - Networking - Need for computer networks - Network Topologies - Types of networks - Hardware needed for setting up simple LAN, Wireless networks and for inter-connecting LANs and WAN - Communication media - Network topologies and access methods - IEEE 802 series standards - Wireless technology - Spread spectrum - WAP and WML - Access points - Service Set ID (SSID) - Authentication methods (OSA, SKA) - Devices used in networking – Hubs – Switches – Routers - Wireless Access Points - Physical connectivity between systems - Types of Cables – Ethernet - Token Ring - Optical Fibre - Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting - Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast

Unit 2: Routing - Fundamentals of routing - Link State Routing - Distance Vector Routing – RIP – EIGRP – OSPF - Configuring Routers - Understanding the router architecture - Assigning IP address to the routers - Configuring routing protocols

Unit 3: Packet Switched Connection - Types of connections – Circuit switched, Packet switched – Importance of Packet Switches - Types of protocols and need for protocols - Packet switched Protocols - TCP/ IP

Unit 4: OSI Layers - Interconnecting disparate systems/ networks – issues - Open Systems Interconnect - 7 layers and their functionality - Introduction to TCP/ IP - Origins of TCP/ IP and evolution of Internet - IP Layers Vs OSI - IP number concepts - Network address - Classes of Networks - Subnet masking - Static and dynamic IP numbers - UDP - Establishing a TCP session (Three way handshake) - Name to address translation - Domain Name System

Unit 5: Networking to the end user - Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - Introduction to ADS (Active Directory Service) - File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server - Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools.

REFERENCES:

1. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
2. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012
3. Network Security: The Complete Reference by Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg, Paperback Edition, McGraw Hill Education, 27 January 2004
4. Cryptography and Network Security by Dr. William Stallings, 6th Edition, Pearson Education Publication, 01 Jan 2013
5. Network Security: Private Communications in a Public World by Mike Speciner, Radia Perlman, Charlie Kaufman, 2nd Edition, Prentice Hall, 22 April 2002

Cyber Crime

Subject Code: **Number of Credits: 04**
Subject Description: This course presents an overview of cyber crimes, trends, frauds and its impact**.**

Goals: The students will be expected to understand various concepts of cyber crimes, trends and forms of cyber crimes and frauds.

Objective: End of this course a candidate will be able to understand:

a. The concepts and definitions of various forms of cyber crimes
b. Current trend in cyber crimes in India and abroad
c. Psychology of cyber crime and cyber criminal and
d. The impact of cyber crimes on various sectors of a country

Contents
Unit 1: Cyber Crime –Definition, Nature and Extent of Cyber Crimes in India and other countries - Classification of Cyber Crimes – Differences between conventional crimes and cyber crimes - Trends in Cyber Crimes across the world.

Unit 2 : Forms of Cyber Crimes , **Frauds** – Cyber bullying, hacking , cracking, DoS – viruses, works, bombs, logical bombs, time bombs, email bombing, data diddling, salami attacks, phishing, stegnography , cyber stalking, spoofing, cyber pornography, defamation, computer vandalism, crimes through social networking sites, malwares, social engineering, credit card frauds & financial frauds, telecom frauds. Cloud based, Ecommerce Frauds and other forms.

Unit 3: Modus Operandi of various cyber crimes and frauds –Modus Operandi **-** Fraud triangle – fraud detection techniques - countermeasures.

Unit 4: Profile of Cyber criminals – Cyber Crime Psychology – Psychological theories dealing with cyber crimes – Learning, Motivation, personality and intelligence theories of cyber criminals – Criminal profiling.

Unit 5: Impact of cyber crimes – Economic, Psychological and Sociological impact on individual, corporate and companies, government and the nation.

REFERENCES:

1. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats by Will Gragido, John Pirc, 1st edition, Syngress, 7 January 2011
2. Cyber Crime & Warfare: All That Matters by Peter Warren, Michael Streeter, Kindle Edition, Hodder & Stoughton, 26 July 2013
3. Digital Evidence and computer crime by Eoghan Casey, 3rd Edition, Academic Press Publication, 17 June 2011
4. The Psychology of Cyber Crime: Concepts and Principles by Grainne Kirwan, Andrew Power, 1 edition, Business Science Reference , 15 March 2012

Network Security

Subject Code: **Number of Credits: 04**
Subject Description: The function of Network Security management includes the management of networks and security systems.

Goals: The students will be expected to understand the function and how they are relevant to security

Objective: On successful completion of the course the student should have understood the Network Architecture, Cabling and Topology, TCP/ IP applications and Network Protocols, Advanced Networking devices, Network Operations

Contents
Unit 1: Network Attacks - IP Attacks, ICMP Attacks, Routing Attacks, TCP Attacks, Application Layer Attacks, Denial of Service Attack, Man-in the Middle Attack

Unit 2: Common Authentication Protocols - Authentication concepts - Various authentication protocols - Password Authentication Protocol (PAP) - Challenge Handshake Authentication Protocol and MS Chap - Extensible Authentication Protocols - Remote Access with RADIUS and TACACS - Single Sign on – Kerberos, SEASAME – Authentication in Wireless networks

Unit 3: Real World Protocols – IPSec, SSL, IKH, AH and ESP - Introduction to IPSec - IPSec building blocks - Security Associations (SAs) - Security Parameter Index (SPI) -IPSec Architecture - IPSec Protocols - Authentication Header (AH) - Encapsulation Security Payload (ESP) - Tunneling and Transport Mode - Internet Key Exchange (IKE) – ISAKMP

Unit 4: Real time Communication Security - IPsec: AH and ESP, IPsec: IKE, SSL/TLS, Firewall, Auditing and intrusion detection

Unit 5: Process& Technology - Email Security, Web Security, Denial of Service, Network Access Control, DDOS Prevention, Intrusion Prevention & Detection System.

REFERENCES:

1. Official (ISC)2 Guide to the CISSP CBK by Adam Gordon, Fourth Edition, (ISC)2 Press, 23 April 2015
2. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
3. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012
4. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
5. Certified Information Systems Security Professional, Study Guide by Ed Tittel, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012

Advanced Information Security

Subject Code: **Number of Credits: 04**
Subject Description: This course provides a comprehensive overview of the essential concepts in Information systems Security

Goals: The students will be expected to understand the Digital Rights introduction, Cryptography, Data base Security and Data Loss Prevention mechanism

Objective: On successful completion of the course the student should have understood the concepts in Information systems Security.

Contents
Unit 1: Digital Rights Management - Meaning of Digital Rights Management (DRM) - Need for DRM and preventing illegal file sharing on the Internet - DRM schemes - Microsoft DRM 2.0, and the Content Scrambling System

Unit 2: **DRM Schemes** – Advantages and disadvantages of DRM schemes - Requirements for a good DRM scheme - secure hardware, secure software, and an efficient legal system

Unit 3: Cryptology - Classical Encryption Techniques - Substitution Techniques - Transposition Techniques –- Permutation Methods - Confidentiality using conventional encryption - Placement of Encryption - Symmetric and Asymmetric crypto systems – common crypto standards and applications - Traffic Confidentiality - Key Distribution - Random Number Generation - Key Management - Generating Keys - Nonlinear Keyspaces - Transferring Keys - Verifying Keys - Using Keys - Updating Keys - Storing Keys - Backup Keys - Compromised Keys - Lifetime of Keys - Destroying Keys - Public-Key Key infrastructure - Criminal Code Systems Analysis - Sports Bookmaking Codes - Horse Race Bookmaking Codes - Number Bookmaking Codes - Drug Codes - Pager Codes- Steganography

Unit 4: Database Security - Overview of Database - Database application security models - Database auditing models - Application data auditing - Practices of database auditing

Unit 5: Data Loss prevention - Content Filtering - Device Control - Network DLP - Host DLP.

REFERENCES:

1. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
2. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012
3. The World Beyond Digital Rights Management by Jude Umeh, 1st edition, BCS - The Chartered Institute for IT, 2009
4. Cryptography and Network Security by Dr. William Stallings, 6th Edition, Pearson Education Publication, 01 Jan 2013
5. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
6. Certified Information Systems Security Professional, Study Guide by Ed Tittel, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012

Digital Forensics tools

Subject Code: **Number of Credits: 04**
Subject Description: This course provides the extensive explanation of the tools, understand the technology better

Goals: It helps the students to explain the use of these tools on Linux and Windows systems as a platform for performing computer forensics

Objective: On successful completion of the course the student should have understood the in-depth analysis and explanation of the software with related applications.

Contents
Unit 1: The Practice of Digital Forensics –Understanding OS file system - Boot process - Hard Drive architecture

Unit 2: OS Forensics – Basic Windows / Linux Forensics including log analyser - Register viewer - Process viewer - Browser logs review - Packet capturing - Password identification.

Unit 3: Forensic Imaging Process –Acquiring the Digital Evidence – Understanding Data Acquisition, Data Acquisition methods and Process

Unit 4: Digital Forensics with Open Source Tools – Digital Forensics – Open Source tools – Benefits of Open Source Tools – Open Source Examination Platform – Preparing the Examination System – Using Linux as the host - Using Windows as the host

Unit 5: Disk and File System Analysis – Media Analysis Concepts – The Sleuth Kit – Partioning Disk Layouts – Special Containers – Hashing – Carving – Forensic Imaging.

REFERENCES:

1. Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey, Paperback – Import Edition, Syngress, 24 May 2011
2. Understanding Forensic Digital Imaging by Herbert L. Blitzer, Karen Stein-Ferguson, Jeffrey Huang, 1st Edition, Academic Press, 26 July 2010
3. The basics of Digital Forensics by John Sammons, 2nd Edition, Elsevier Publication, 2012
4. Windows Forensics Analysis Tool kit by Harlan Carvey, 3rd Edition, Syngress Publication, 2007
5. Cyber Forensics: A field manual for collecting, Examining, preserving evidence of computer crimes by Albert Marcella, Jr., Doug Menendez, Second Edition, CRC Press 2007
6. Encase Computer Forensics – The Official EnCE: Encase Certified Examiner Study Guide by Steve Bunting, 3rd Edition, John Wiley & Sons Publication, 2012

Threats in Social Media

Subject Code: **Number of Credits: 04**
Subject Description: This course presents an analysis of the concepts of information security followed by a discussion of threats, impact, computer security, information security, network security, personal privacy and informational privacy

Goals: It helps the students to understand the cyber threats in social media

Objective: On successful completion of the course the student should have understood the cyber threats in Social websites, classify their types, discuss the cyber threats and its impact

Contents
Unit 1: Media & Journalism - Overview – History, Types , advantages and disadvantages of various media – Journalism – Types of Journalism, Investigative Journalism – Yellow Journalism – Ethics of a Journalist

Unit 2: Social Media – Print and Television media – Social Networking Sites, Types, advantages and disadvantages, Social Media ethics – Do's and Dont's in various social medias

Unit 3: Victimization in social media – Types of victimization – Profiles of social media victims - causes of victimization – trends in victimization in social media in India and other countries.
Impact of Social Media threats - Harm to Brand Reputation - Lost Productivity - Strains on Bandwidth - Data Leaks & Disclosure

Unit 4: Threats against Organizations from Social Media - Executive impersonations - Account takeover - Watering hole phising and malware - Customer scams - Corporate impersonations - Information Leakage - Planning of an attack - Clickbait attacks - Hashtag/ traffic Hijacking

Unit 5: Social media security policies – individuals - Organizational Security Policies – Safe surfing - Safe Message Handling - Anti-Malware Software - Privacy Policies -Safe Browsing practices

REFERENCES:

1. Security in the Digital Age: Social Media Security Threats an Vulnerabilities by Henry A. Oliver, Paperback – Import Edition, CreateSpace Independent Publishing Platform, 11 August 2015
2. Threats and anti threats Strategies for Social Networking Websites by Amir Rokiifard, volume 5, International Journal of Computer networks and Communications, July 2013
3. Securing the Social Media in the Enterprise by Henry Dalziel, 1st Edition, Elsevier Publication, 2015
4. Securing the Clicks: Network Security in the Age of Social media by Gary Bahadur, Jason Inasi, Alex de Carvalho, Illustrated Edition, Mc. Graw Hill Professional Publication, 2011
5. Policing Cyber Crime: Networked and Social Media Technologies and the challenges for Policing by David S Wall, Matthew L Williams, 1st Edition, Routledge Publication, 16 May 2014

Mobile Security

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with the overview of mobile device security, Understanding attack Hackers.

Goals: The students will be expected to understand the Mobile Device Security, Vulnerabilities, Threats and Countermeasures

Objective: On successful completion of the course the student should have understood

a. Mobile device monitoring
b. Identifying the threats
c. Ensure the safety of the mobile device
d. Recover from being hacked
e. Deal with a compromised or lost device

Contents
Unit 1: Mobile Issues and Development Strategies – Physical Security – Strong authentication with poor keyboards – Safe browsing environment – Secure Operating Systems – Application Isolation – Virus, Worms, Trojans, Spyware and malware - Insecure Device drivers

Unit 2: Android Security - Developing and debugging on android – Androids Securable IPC mechanisms – Androids Security Model – Android Permissions Review – Content Providers – Mass storage - Android Security tools

Unit 3: Vulnerabilities, Threats of Mobile Devices and Countermeasures - Understanding Attack vectors, Overview of various Mobile Malwares, Network Attacks, Mobile malware defenses: Advantages and disadvantages, Protect against Mobile Malware, Protect against identity theft, Protect against Mobile DoS (Denial of Service Attacks), Protect against Bluetooth attacks

Unit 4: Mobile malware – Important post malware – Threat Scenarios – mitigating mobile malware – For developers and platform vendors

Unit 5: Mobile Security Penetration Testing tools – Mobile platform attack tools and utilities – browser extensions – networking tools – Web application tools

REFERENCES:

1. Mobile Application Security by Himanshu Dwivedi, 1st Edition, McGraw-Hill Education, February 5, 2010
2. Wireless and Mobile Device Security by Jim Doherty, 1st Edition, Jones and Barlett Publication, 2014
3. Mobile Security: How to Secure, Privatize, and Recover your devices by Timothy Speed, Darla Nykamp, Mary Heiser, Joseph Anderson, Jaya Nampalli, reprint edition, Packt Publication, 2013
4. Mobile Device Security: A comprehensive guide to securing your Information in a Moving World by Stephen Fried, illustrated edition, Taylor & Francis Publication, 2010

IT Governance, Risk and Compliance

Subject Code: **Number of Credits: 04**
Subject Description: This course provides the students to learn how to manage business risks, governance and compliance

Goals: The students will be expected to understand the best Practices of IT Governance, ISMS and Compliance

Objective: On successful completion of the course the student should have understood

a. Developing Strategic metrics
b. Defining roles and responsibilities
c. Establishing risk management objectives
d. Steps for implementing an effective strategy

Contents

Unit 1: Governance, Risk & Compliance GRC – Definitions – Governance, Risk, Compliance, Risk Threshold, Risk Modeling, Risk Appetite, Governance Standards

Unit 2: Best Practices for IT Governance – ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) - The Information Security Management Maturity Model - Capability Maturity Model – latest standards and compliance technologies.

Unit 3: Information Security Governance - Effective Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment - Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee - Policies and Procedures

Unit 4: Information Security Management Practices - Personnel Management - Financial Management – Quality Management - Information Security Management - Performance Optimization - Roles and Responsibilities - Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools - Case Study Analysis - Risk Management framework – COSO - The Internal environment - Objective Setting - Event Identification - Risk assessment - Risk Response - Control activities - Information & communication – Monitoring – NIST - Risk Assessment - Risk Mitigation - Evaluation & Assessment - Case Study Analysis

Unit 5: Compliance – Introduction - Information Technology and security - Evolution of Information systems - Roles and responsibilities - Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - Compliance officer activities - The requirements of a Compliance Officer - Drafting compliance reports - Designing an Internal Compliance System - Regulatory principles – Issues - Developing high-level compliance policies - Defining responsibility for compliance - The compliance function - Specific internal compliance control issues – Information System Audit - Scope of System Audit - Audit Planning - Audit Manual - Audit check lists - Audit Reports - Best Practices for IT compliance and Regulatory Requirements

REFERENCES:

1. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby, 1st Edition, Wiley Publication, 13 April 2009
2. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition by W. KragBrotby, 2nd Edition, ISACA Publication, 01 Mar 2006
3. Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture by Fred Cohen, Large Print Edition, Fred Cohen & Assosciates Publication, 2005
4. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
5. IT Compliance and Controls: Best Practices for Implementation by James J., IV DeLuccia, Illustrated Edition, Wiley Publication, 2008
6. The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments by Craig S. Wright, Brian Freedman, Dale Liu, 1st Edition, Syngress Publication, 2008
7. Auditor's Guide to Information Systems Auditing by Richard E. Cascarino, 2nd Edition, Wiley Publication, 03 Apr 2012
8. COBIT 4.1 – Available at www.isaca.org
9. www.sarbanes-oxley.com

Business Continuity Planning (BCP) and Disaster Recovery (DR)

Subject Code: **Number of Credits: 04**
Subject Description: The course deals with two domains in one: BCP is about making the plans and creating the framework to ensure that the business can continue in an emergency; DRP is about quickly recovering from an emergency with the minimum of impact to the organization.

Goals: The student should understand the following:

a. The basic difference between BCP and DRP
b. The difference between natural and manmade disasters
c. The four prime elements of BCP
d. The steps in conducting a Business Impact Assessment (BIA)
e. The steps in creating a disaster recovery plan
f. The five types of disaster recovery plan tests
g. The various types of backup services

Objective: On successful completion of the course the student should know the concepts behind Business Continuity Planning and Disaster Recovery

Contents
Unit 1: Introduction - Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR) - Terms and definitions - BCM principles - BCM lifecycle - (BCM programme management, Understanding the organization - Determining business continuity strategy, Developing and implementing a BCM response, BCM exercising, Maintaining and reviewing BCM arrangements, Embedding BCM in the organization's culture) - BCM in business: Benefits and consequence - Contemporary landscape: Trends and directions

Unit 2: Business Impact Analysis - BCM and DR – The relationship with Risk Management - Risk Management concepts and framework - Concepts of threat, vulnerabilities and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting - Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting - Relationship between BIA and Risk Management

Unit 3: Business Continuity Strategy and Business Continuity Plan (BCP) Development - Business continuity strategy development framework - Cost-benefit assessment - Site assessment and selection - Selection of recovery options - Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies - Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools

Unit 4: Business Continuity Plan Testing and Maintenance - Test plan framework - Types of testing - Business Continuity Plan Testing - Plan maintenance requirements and parameters - Change management and control - Business Continuity Plan Audits

Unit 5: Disaster Recovery – Definitions - Backup and recovery - Threat and risk assessment - Site assessment and selection - Disaster Recovery Roadmap - Disaster Recovery Plan (DRP) preparation - Vendor selection and implementation - Difference between BCP and DRP - Systems and communication security during recovery and repair

REFERENCES:

1. BS25999-1:2006 (BSI)
2. Business Continuity Planning: A Step-by-Step Guide With Planning Forms on CD-ROM by Kenneth L. Flumer, 3rd edition, Rothstein Associates Publication, 04 Oct 2004
3. A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance by Julia Graham, David Kaye and Philip Jan Rothstein, Illustrated edition, Rothstein Associates Publication, 31 Jan2006
4. Business Continuity Planning – Protecting Your Organization's Life by Ken Doughty, Illustrated edition, Taylor & Francis Publication, 2000
5. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
6. The Definitive Handbook of Business Continuity Management by Andrew Hiles, 3rd Edition, John Wiley & Sons Publication, 22 Oct 2010
7. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002
8. Certified Information Systems Security Professional, Study Guide by Ed Tittel, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012

Cloud Computing

Subject Code: **Number of Credits: 04**
Subject Description: The course provides the coverage of cloud computing environments, Cloud Application, Legal and Compliance requirements Security

Goals: The students will be expected to understand cloud computing which has been deployed within every function in a broad range of business and enterprises

Objective: On successful completion of the course the student have understood the benefits of Cloud Computing

Contents
Unit 1 – Fundamentals of Cloud Computing, Cloud Platforms / Categories, Cloud Components, Virtualization

Unit 2 – Cloud Deployment Model, Data Center requirements for hosting Cloud Infrastructure, Common Threats, Security Considerations for various Cloud Categories, Cloud Security Data Lifecycle

Unit 3 – Cloud Platform and Infrastructure Security – Security Requirements of Cloud Infrastructure: Network – Virtualization – Storage - Physical and Environmental

Unit 4 – Cloud Application Security with respect to Access Control – Identity and Access Management, Federation, Multifactor Authentication. OWASP and SANS recommendation of Cloud Security requirements

Unit 5 – Best practices and the future of cloud computing – Establishing a baseline and metrics – Phased in vs flash cut approaches – Researcher predictions – Responding to change

REFERENCES:

1. Cloud Computing, A Practical Approach by Toby Velte, Anthony Velte, Robert C. Elsenpeter, 1st Edition, McGraw-Hill Education, 1 November 2009
2. Cloud Computing Bible: A Practical Approach to Cloud Computing Security, Cloud Problems To Be Aware of and More by Denise Gonzales, Kindle Edition
3. Cloud Computing: Methods and Practical Approaches (Computer Communications and Networks) by Zaigham Mahmood, 2013 edition, Springer, 4 June 2013
4. The basics of Cloud Computing – Understanding the fundamentals of cloud computing in theory and practice by Derrick Rountree, Ileana Castrilo, Illustrated Edition, Syngress Publication, 01 Nov 2013

ELECTIVES

Cyber Law

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with the Fundamentals of Cyber Law, crime Investigation and the legal issues

Goals: The goal of this course is to make a student understand the legal and other supplementary provisions relating to cyber crimes and technology related crimes.

Objective: End of this course a candidate will be able to understand:

a. The fundamentals of cyber crimes
b. Provisions relating to E-Governance and E-Commerce
c. Procedures and powers relating to investigation of a cyber crime
d. Legal issues relating to courtroom practices and
e. Case laws dealing with cyber crimes

Contents

Unit 1: Fundamentals of Cyber Law - Introduction on cyber space - Jurisprudence of Cyber Law - Scope of Cyber Law - Cyber law in India with special reference to Information Technology Act, 2000 (as amended) and Information Technology Act, 2008 – Jurisdiction issues in Cyberspace-Theories in cyber law jurisdiction – Cybercrimes -Meaning and Types.

Unit 2: E- Governance and E – Commerce - Electronic Governance – Procedures in India - Essentials & System of Digital Signatures - The Role and Function of Certifying Authorities - Digital contracts – Validity of Electronic Contract-Types of Electronic Contract - UNCITRAL Model law on Electronic Commerce - Cryptography – Encryption and decryption –Legal Issues In E banking transactions.

Unit 3: Cyber Crimes Investigation - Investigation related issues - Issues relating to Jurisdiction in investigation and enforcement – Powers and function of Investigating officials-Search and Confiscation-Issues in Cross Border Investigation-Coordination among nations for cybercrime investigation -Relevant provisions under Information Technology Act, Indian Evidence Act, Indian Penal Code - Cyber forensics - Case studies.

Unit 4: **Legal Issues and Courtroom Skills -** Key legal aspects of computer crime - IT Act of 2000 and amendments – Evidentiary issues in trial of cybercrime cases - Overseas Co-operation in Cyber Terrorism prevention - Seizure of backups and data Disclosure - Selected comparative law overseas - Civil Issues and General Enforcement - Potential defamation - Intellectual Property infringements - Confidentiality Obligations - Data Preservation and Retention - Seizure of Records - Proceeds of Crime - Damages - The domain of the Instrument of Fraud - Evidential aspects of computer material - Planning operations - Admissibility - Discovery – civil and criminal - Particular Devices - Best Practice - Preparation of Material for Court - Challenges and suggested solutions - Evidential presentation and explanation - Key players in the courtroom - Role, obligation and expectations of an 'expert witness' –Online Arbitration –Cyber Regulation Appellate Tribunal.

Unit 5: **Practices in Cyber Jurisprudence** – Regional and Global - Important Case Laws in India and other countries – Need for International cooperation for cybercrime investigation and enforcement-Need for separate cyber court - cyber laws in other countries.

REFERENCES:

1. Cyber law by Nandan kamath, Fifth Edition, Universal law Publication, 01 Jan 2012
2. Intellectual property by Robert P Merges, 3rd Edition, Aspen Publication, 2003
3. Computers , Technology and the new internet laws by Karnika Seth, Updated Edition, Lexis nexis Publication, 01 Jan 2013
4. Legal dimensions of cyber space by S.K.Verma, Volume 1, Ashgate Publication, 01 Jan 2001

Cyber Criminology

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with the fundamentals of cyber Criminology

Goals: The goal of this paper is to make a student learn the basic concepts of Criminology and thereby Cyber Criminology

Objective: End of this course the students will be able to appreciate the

a. Sociological and Criminological Perspectives and theories of Cyber Criminology
b. Understand the contemporary forms of crimes
c. Basic concepts of Criminology and
d. The role of the Criminal Justice System and victims in the prevention of cyber crimes.

Contents
Unit 1 : Principles and Concepts of Cyber Criminology – Crime, Tort, Misdemeanor, Cyber Space, Cyber Crime, Cyber Criminology, Information Security, Penetration Testing, Incident Response, GRC
- Conventional crimes vs Cyber Crimes.

Unit 2: Contemporary Forms of Crimes - White Collar Crimes, Economic Offences, Organized Crimes, Terrorism, Crime and Media and other contemporary forms of crimes.

Unit 3 : Cyber Crime – Sociological and Criminological Perspectives – Causes of Cyber Crimes - Criminological Theories and Cyber Crime – Routine Activity Theory, Social Learning Theory, Differential Association Theory, Differential Opportunity Theory, Media and Crime and latest theories and other related theories.

Unit 4: The Role of Police and Cyber Crimes - Police – Organizational structure of Police in India – Different wings in the States and Districts and their functions - Police & Law Enforcement – F.I.R. – cognizable and non-cognizable offences, bailable and non-bailable offences – arrest , search, seizure – Interrogation of suspects and witnesses – charge sheet – Intelligence system- Gathering intelligence, gathering evidence – oral, documentary and circumstantial – Police Act, 1861 – National Police Commission Reports (Modernization of Police) - Cyber crime cells – structure & functions, issues and problems in the investigation of cyber crimes cases – Important Case Studies.

Unit 5: **The Role of Judiciary and N.G.O.s and Cyber Crimes**: Judiciary - Different types of courts – Cyber Appellate Court / Tribunals / Powers – Proceedings in the court before trial, after trial, plea of guilty, sentencing - The Role of N.G.O.s in the Prevention of Cyber Crimes – Cyber Crime Victims – Impact of Cyber Crimes on Victims, The Role of Victims of Cyber Crimes in the Criminal Justice Administration

REFERENCES:

1. Cyber Criminology: Exploring the internet crimes and criminal behavior by K. Jaishankar, Illustrated Edition, CRC Press, 2011
2. Cyber Law: Law of Information Technology and Internet by Anirudh Rastogi, L.L.M Harvard, 1st Edition, Lexis nexis Publication, 01 Sep 2014
3. Computer Forensics and Cyber Crime by Britz M T , 3rd Edition, Pearson Education Publication, 2013
4. Cyber Crime: Issues, Threats and management by Jain Atul, 1st Edition, Isha books Publication, 15 Nov 2014

Intellectual Property Rights

Subject Code: **Number of Credits: 04**
Subject Description: This course deals with an overview of Intellectual Property Rights

Goals: The goal of this paper is to make a student learn the basic concepts of IPR, Patents, Trade marks, Copyright and industrial designs

Objective: End of this course the students will be able to understand the

a. Concept of intellectual Property and the need for protection
b. Salient features of Patents and Trade Mark
c. The Copyright Act (1957) and recent amendments
d. Industrial Designs

Contents

Unit 1 - Intellectual Property - Meaning and concept of intellectual Property and the need for protection - The world Intellectual property Organisation (WIPO) Convention - Origin and functions of World Trade Organisation (WTO) - Trade Related Intellectual property Rights (TRIPS) Agreement of WTO and its effects on Intellectual Property law in India; Dispute Settlement Mechanism.

Unit 2: **Patents -** The Patents Act O(1970), object definitions, salient features, patentable and non- patentable inventions, product and process patents –Patent applicants, provisional and complete specifications, priority dates, of claims, opposition to grant of patent, anticipation, provisions for secrecy of certain inventions - Patent office and power of Controller - Grant and sealing of patents, rights of patentees, rights of co-owners of patents, term of patent, patents of addition, assignment and transmission, register of patents - Amendment of applications and specifications, restoration of lapsed patents, rights of patentees of lapsed patents, surrender and revocation of patents - Compulsory licences, exclusive marketing rights, licences of right, use of invocation of patents purposes of government, acquisition of inventions by Central Government - Remedies for infringement of patents - Patent agents, scientific advisers, international arrangements - Right of plant breeders and farmers - National Law on Biological Diversity

Unit 3 - Trade Marks - The Trade Mark Act (1999), object, definitions, salient features, marks registrable and non – registrable, conditions for registration, absolute and relative grounds for refusal of registration, procedure for and duration of registration, effects of registration - Powers and functions of Registrar - Distinctiveness, deceptive similarity, concurrent registration, rectification and correction of register - Assignment and transmission - Use of trademarks and registered users, collective marks, registration of certification mars, trade mark agents - Appellate board - Infringement action, passing off action - International treaties.

Unit 4 - Copyright - The Copyright Act (1957) and recent amendments: works in which copyright subsists - meaning of copyright ; ownership and rights of the owner; assignment; term of copyright - Registration of copyright; compulsory licences - copyright societies - Rights of broadcasting organisations and of performers - International copyright - Acts constituting & not constituting infringement; remedies for infringement

Unit 5: Industrial Designs - The designs Act, 2000 - definitions, registration of designs, copyright in registered designs, piracy of registered designs, remedies, powers and duties of Controller, International Law - Semi conductor integrated circuit layout – Design Act – 2000

REFERENCES:

1. Law relating to patents, trademarks, copyright, design and geographical indications by Dr. B.L. Wadehra, 5th edition, Universal law Publication, 2012
2. Law of Intellectual Property by Dr. S.R. Myneni, 6th Edition, Asia Law House Publication, 01 Jan 2013
3. International Property by David I. Bainbridge, 9th Edition, Pearson Education Publication, 24 May 2012
4. Intellectual Property, Patents, Copyright, trademarks and allied rights by W.R. Cornish, D Llewelyn, 6th Edition, sweet and Maxwell Publication, 18 June 2007

E-mail forensics

Subject Code: **Number of Credits: 04**
Subject Description: This course provides the detailed application of forensic analysis techniques to the field of email Security

Goals: It describes roles and responsibilities of different email actors and components and itemizes meta data contained in email headers and lists protocols and ports used in it

Objective: On successful completion of the course the student should have understood both investigative and preventative techniques but the focus is on prevention

Contents
Unit 1: Introduction to Email Forensics – Basic concepts – Email, Headers, IP address, IP locators, Email threads, functioning of an E-Mail, E-Mail investigation, E-Mail recovery – Email Service Providers , anonymous emails, fake emails and spam emails.

Unit 2: Email Actors, Roles and Responsibilities – User Actors, Message handling Service (MHS) Actors, Administrative Management Domain (AMD) actors

Unit 3: Email Identities and Data - e-mail messages, contacts, tasks, calendars, account settings, Scrapbook clips – creating and deleting identities, importing and exporting identities, importing and exporting contacts and other details from different emails, risks of cloud storage in E-Mails, phishing, identity theft and data theft from emails and attachments.

Unit 4: Email Forensic Investigation Techniques – Header Analysis, Bait tactics, Server Investigation, Network Device Investigation – Software Embedded Identifiers – Sender Mailer Fingerprints

Unit 5: Email Forensics Tools – eMail Tracker Pro - eMail Tracker – Adcomplain - Aid4mail forensic – Abuse pipe, Access data's FTK, Encase Forensics, FinaleMail, Sawmill Groupwise, Forensic Investigation Toolkit – Paraben (Network) Email Examiner.

REFERENCES:

1. Email Forensics: Eliminating Spam, Scams, and Phishing by Les Hatton, Illustrated Edition, Blue spear Publication, 28 Oct 2011
2. The basics of Digital Forensics by John Sammons, Second Edition, Syngress Publication, 02 April 2012
3. International Journal of Network Security & its application – M. Tariq Banday
4. Journal of Information Security, A comprehensive study of Email Forensic tools – Vamshee Krishna Devendra, Hossain Shahriar, Victor Clincy

Digital Frauds

Subject Code: **Number of Credits: 04**
Subject Description: This course deals where fraud and misconduct threaten and key signs of fraud in financial statements

Goals: The goal is to provide proven approaches to customize a strategy for preventing, detecting, and responding to fraud and corruption by building a culture of ethics and integrity

Objective: It helps the students by providing guidance on how to

a. Access organizations vulnerability to fraud and misconduct, design and implement controls to prevent, detect, and respond to these occurrences
b. Address increased regulatory enforcement and enhanced scrutiny
c. Preserve and create value from corporate governance and compliance programs
d. Use technology and data analytics to mitigate fraud and misconduct risks
e. Evaluate the ongoing effectiveness of your compliance program

Contents
Unit 1: Fundamentals of Frauds - Definition of fraud, fraud risk management, fraud taxonomy, fraudulent behavior, red flags

Unit 2: Banking Frauds – Authentication Management, Payment Fraud, Fraud Consulting and Services, Card & Emerging Payments Fraud, Contact Center Fraud Prevention, Cheque Fraud, Internal Threats,

Unit 3: Corporate Frauds – What is Corporate Frauds – Services - Solutions

Unit 4: Financial Frauds – Financial Inclusions and mobile financial Services, Regulating for financial inclusions, Agent network issues, Telecommunication access network issues, Account to account interoperability issues, Customer data and risk based financial issues, Consumer Protection, Collaboration among financial, telecommunications and competition authorities

Unit 5: Frauds in IT and Telecom - IT Frauds: Theft of Proprietary Information, Insider abuse of internet access, system penetration, unauthorised access to information, laptop/mobile theft, financial fraud, misuse of public web application, virus, abuse of wireless network – Countermeasures – Telecom Frauds - Organizational or Non-Technical Fraud: involving Administration services, processes - Human Fraud - Insider Fraud - Call-sell Fraud - Facilitation Fraud - Creeping Fraud - Chaining Fraud - Calling-Card Fraud - Phantom Account - Partnership Fraud - Process Fraud – Ghosting - Abuse of test or emergency lines or accounts - Unauthorized Feature/Service Activation – Accounting - Dealer or Reseller Fraud - Subscription Fraud - Roaming Subscription Fraud - Premium-Rate Services Fraud- Illustrative Cases - Technical Fraud: Network Systems, Billing Systems – Cloning – Tumbling - Voice-mail Hacking - PBX Hacking - SIM Stuffing- Clip-on Fraud - Line Tapping - War Dialing - Handset Fraud – Fixed Network Fraud – Mobile Network Fraud – Frauds in 2G, 3G and 4G Frauds

REFERENCES:

1. Managing the risk of fraud and misconduct by Richard H Girgenti, and Timothy P Hedley, first edition, Mc Graw Hill Education Publication, 09 Mar 2011
2. Detecting Accounting Fraud: Analysis and Ethics by Cecil W Jackson, 1st Edition, Pearson Education Publication, 26 Jan 2014
3. Anatomy of a fraud investigation by Stephen Pedeault, 1st Edition, John Wiley & Sons Publication, 2010
4. Telecom and Network Security: Toll Fraud and Telabuse update by Jan Wilson, 2nd Edition, Telecommunications reports International Publication, 22 April 2010