NOTIFICATION

No. 118 /2023 Date : 17/08/2023

Subject: Implementation of new Syllabus of Semester I & II of the new Course P.G. Diploma in Cyber Security [One Year Two Semesters (CBCS) Course] as per CBCS guidelines.

It is notified for general information of all concerned that the authorities of the University have accepted to implement the new Syllabus of Semester I & II of the new Course P.G. Diploma in Cyber Security [One Year Two Semesters (CBCS) Course] as per CBCS guidelines to be implemented from the academic session 2023-2024 & onwards as given below:

Sd/-
(Dr.T.R.Deshmukh)
Registrar

Syllabus Prescribed for Semester I & II of the new Course P.G. Diploma in Cyber Securuty (CBCS)

SEMESTER I

1PGDCY00 INTRODUCTION TO COMPUTERS

Course Objective: Throughout the course, students will be expected to demonstrate their understanding ofFundamentals of Computers, Operating Systems, Computer Networks, Internet, Office andProgramming Concepts by being able to do each of the following:

To understand the basic terminology used in Computers, Operating Systems andComputer Networks, Internet, concept of Office, concepts of Programming.

Course Outcomes (Expected Outcome): After Successful completion of this course, the studentwould be able to:

1. Identify the basic concepts and technologies involved in dealing with Computers.
2. Understand different types of Operating Systems.
3. Apply and use different technologies for Computer Networks, Internet and WebBrowsers, Office and the Programming Concepts.

Unit I: Introduction to Computers:
Definition and components of a computer system, Types of computers, Classification of computers, based on size, purpose, and generations, Computer applications in various fields.

Unit II: Operating Systems:
Definition and functions of an operating system, Types of operating systems (e.g., Windows, macOS, Linux), File management and system utilities, User interface and customization

Unit III: Computer Networks:
Definition and types of computer networks, Network topologies and protocols, Network devices and their functions (e.g., routers, switches, hubs), Internet and World Wide Web,

Unit IV: Internet and Web Browsers:
Definition and history of the Internet, Web browsers and their features, Search engines and their operations, Internet security and privacy issues,

Unit IV: Microsoft Office Suite:
Introduction to Microsoft Office Suite (Word, Excel, PowerPoint, and Access), Features and functions of each application, Creating and editing documents, spreadsheets, presentations, and databases, Data analysis and visualization

Unit VI: Programming Basics:
Introduction to programming concepts and languages, Programming logic and algorithms, Variables, data types, and operators, Control structures (e.g., conditional statements, loops),

Text Books:

1. "Computer Fundamentals" by Pradeep K. Sinha and Priti Sinha (BPB Publications).
2. "Introduction to Computers" by V. Rajaraman (PHI Learning Private Limited).

Reference Books:

1. "Computer Science with Python: Textbook for CBSE Class 11" by Sumita Arora (Dhanpat Rai Publications).
2. "Introduction to Computers and Programming in C" by Sanjay Saxena (S.K. Kataria& Sons).
3. "Basics of Computers" by S.K. Bhushan and S. Suresh Kumar (I.K. International Publishing House Pvt. Ltd.).
4. "Discovering Computers" by Misty E. Vermaat, Susan L. Sebok, and Steven M. Freund.
5. "Computer Science: An Overview" by J. Glenn Brookshear and Dennis Brylow.

1PGDCY 01 CYBER LAW - I (L-4, T-0, P-0, C-4)

Course Prerequisite: Introduction to Computers

Course Objectives: Throughout the course, students will be expected to demonstrate their understanding ofCyber Law by being able to do each of the following

1. To understand various key paradigms for Cyber Law and Cyber Crimes.
2. To familiarize with the Information Technology Act 2000 and Investigations in CyberCrimes.
3. To understand Human Rights Perspective of Cyber Crimes, Precautions and Preventions.

Course Outcomes (Expected Outcome): After Successful completion of this course, the studentwould be able to:

1. Understand fundamentals of Cyber Crime and Cyber Law
2. Describe Impact of IT Act and Forms of Cyber Crimes
3. Understand Computer and Cyber Crimes in Indian Perspective
4. Understand Role of IT Act and Investigations in Cyber Crimes.
5. Understand Cyber Crimes Evidences and its preventions.
6. Understand Human Rights Perspective of Cyber Crime and its Prevention andPrecautions.

Unit I: Information Technology and Cyber Crimes: (Hours-07) Information Technology and Cyber Crimes: An Introduction, Information Technology:Definition& Perspectives, Growth & Future, Dimensions and Influence on Lives.

Unit II: Regulatory Perspectives & Technology, Forms of Cyber Crimes: (Hours-08)
Impact of Information & Technology, Regulation of Cyber Space, Legal Aspects of Regulation, Influence of Technology on Criminality, Forms of Cyber Crimes.

Unit III: Computer & Cyber Crimes, Indian Response: (Hours-08)
Computer & Cyber Crimes: Terminological Aspects, Opportunities to Cyber Criminals, Motives of Offenders, Problems affecting Prosecution, Cyber Crime: challenges and prevention control, Need and prospects of Criminological Research, Indian Information Act 2000, Preamble & Coverage, Nature of Offences and Penalties, Future Prospects and Needs.

Unit IV: Mens Rea and Criminal Liability, Investigations in Cyber Crimes (Hours-09)

Introduction, Historical Perspectives, Mens Rea in Indian Criminal Law, Abetment of Offence, Criminal Liability and Role of Mens Rea in Indian Information Technology Act 2000, Investigations in Cyber Crimes: Implication and Challenges, Introduction, Procedural Aspects, Issues, Complications & Challenges concerning Cyber Crimes, Problems and Precautionary measures for Investigations.

Unit V: Cyber Crimes: Discovery and Appreciation of Evidences, Prevention Hours-09 Introduction, Law of Evidence: An Introduction, Evidences in Cyber Crime: Challenges and Implications, Computer Generated Evidences and their Admissibility, Judicial Interpretations of Computer related Evidence, Prevention of Cyber Crimes: Introduction, International Services on Discovery and Recovery of Electronic and Internet Evidence, IOCE, OECD Initiatives, Efforts of G& and G8 Groups, Efforts of WTO, WIPO, Interpol and its measures, Efforts in India.

Unit VI: Human Rights Perspectives in Cyber Crimes, Precaution and PreventionHours-07 Introduction, Ideological Aspects, Fundamental rights and Civil Liberties, Various Issues and Challenges, Cyber Crime Precaution and Prevention: Introduction, Awareness and Law Reforms,Improving Criminal Justice Administration, Increasing International Cooperation, CurricularEndeavours and Checking Kids Net Addiction, Role of Guardians, Mobile Pornography, Self Regulation in Cyber Space.

Text Book:
Dr Pramod Kumar Singh, Book Enclave, Jaipur, India, ISBN: 978-81-8152-163-7 “Laws on Cyber Crimes”.

Reference Books:

1. Rahul Sharma, "Cyber Law: Indian Perspective"
2. Pawan Duggal, “Text Book on Cyber Law”, Universal Law Publishing, Second Edition,2016
3. Prashant Mali, “Cyber Law and Cyber Crimes Simplified”, Cyber Info media, 2017
4. Dr. R. K. Bangia "Cyber Law and Information Technology Act"
5. Vakul Sharma "Information Technology Law and Practice"
6. Dr. P. V. S. Jagan Mohan Rao "E-Commerce and Cyber Laws"
7. Jonathan Rosenoer "Cyber Law: The Law of the Internet and Information Technology"
8. Vivek Sood "Cyber Law Simplified"
9. Andrew Murray "Information Technology Law: The Law and Society"

1PGDCY 02 INTRODUCTION TO CYBER SECURITY (L-4, T-0, P-0, C-4)

Course Pre-requisite: Introduction to Computer & Computer Programming, Cyber Law

Course Objectives: Throughout the course, students will be expected to demonstrate theirunderstanding of Introduction to Cyber Security by being able to do each of the following:

1. Understand basics of Cybercrime and Information Security.
2. To familiarize various cyber threats, attacks, Cyber offenses.
3. Understand Cybercrime on Mobile and Wireless devices.
4. Understand tools and methods used in Cybercrime.
5. Understand Access Control and Authentication.
6. Understand Intrusion Detection and Prevention.

Course Outcomes (Expected Outcome): After completion of this course, the students would beable to:
1. Know fundamentals of Cybercrimes and Cyber offenses
2. Realize the Cyber threats, attacks and Vulnerabilities.
3. Explore the industry practices and tools.
4. Comprehend the Access Control and Authentication Process.
5. Implement Intrusion Detection and Prevention.

Unit I: (Hours-08)
Introduction to Cyber Crime: Introduction, Cybercrime, Cybercrime and Information Security, Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era.

Unit II: (Hours-08)
Cyber offenses: Introduction, Attacks, Social Engineering, Cyber stalking, Cyber cafe and Cybercrime, Botnets, Attack Vector, Cloud Computing.

Unit III: (Hours-08)
Cybercrime: Mobile and Wireless Devices Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Cards Frauds in Mobile and Wireless Computing, Security Challenges posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implementations for Organizations, Organizational Measures for Handling Mobile, Devices Related Security Issues Organizational Security Policies and Measures in Mobile Computing, Laptops.

Unit IV: (Hours-08)
Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks onWireless Networks.

Unit V: (Hours-08)
Access Control and Authorization: Definitions, Access Rights, Access Control Systems, Authorization, Types of Authorization Systems, Authorization Principles, Authorization Granularity, Web Access and Authorization.
Authentication: Definition, Multiple Factors and Effectiveness of Authentication, Authentication Elements, Types of Authentication, Authentication Methods.

Unit VI: (Hours-08)
System Intrusion Detection and Prevention: Definition, Intrusion Detection, IntrusionDetection Systems (IDSs), Types of Intrusion Detection Systems, The Changing Nature of IDSTools, Response to System Intrusion, Challenges to Intrusion Detection Systems, Implementingan Intrusion Detection System, Intrusion Prevention Systems (IPSs), Intrusion Detection Tools.
Disaster Management: Introduction, Disaster Prevention, Disaster Response, Disaster Recovery, Make your Business Disaster Ready, Resources for Disaster Planning and Recovery.

Text Books:
1. Nina Godbole, Sunit Belapure, “Cyber Security: Understanding Cyber Crimes, ComputerForensics and Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, 2013.
2. Joseph Migga Kizza, “A Guide to Computer Network Security”, Springer 2009.

Reference Books:
1. V.K. Pachghare, “Cryptography and information Security”, PHI Learning Private Limited,Delhi India.
2. Nina Godbole, “Information Systems Security”, Wiley India, New Delhi
3. Kennetch J. Knapp, “Cyber Security & Global Information Assurance”, Information SciencePublishing.
4. James Graham, Richard Howard, Ryan Olson, “Cyber Security Essentials” CRC Press.
5. Jeetendra Pande, “Introduction to Cyber Security” Uttarakhand Open University, 2017.

1PGDCY 03 CYBER CRIMES AND INVESTIGATION PROCEDURES (L-4, T-0, P-0, C-4)

Course Pre-requisite: Cyber Laws, Cyber Security

Course Objectives: Throughout the course, students will be expected to demonstrate theirunderstanding of Cyber Crimes by being able to do each of the following:

1. Understand basics of Cybercrime and Information Security.
2. To get familiarized with various cyber threats, attacks, Cyber offenses related NetworkForensics, Web, Router Forensics, Internet Crimes.
3. Understand Cybercrime on different devices.
4. Understand Corporate Espionage
5. Understand Sexual harassment.

Course Outcomes (Expected Outcome): After completion of this course, the students would beable to:
1. Know fundamentals of Network Forensics and Investigation Logs
2. Investigate Web Attacks.
3. Know fundamentals of Router Forensics and DoS Attacks.
4. Investigate Internet Crimes, Internet Forensics, Emails.
5. Investigate Corporate Espionage
6. Investigate Sexual Harassment and Child Pornography

Unit I: (Hours-08)
Network Forensics & Investigating Logs, Log Files as Evidence, Synchronize Computer TimeInvestigating Networks Traffic, Network Addressing Schemes, OSI Reference Model, Overview of Network Protocols, Types of Networks Attacks, Evidence Gathering, DNS Poisoning Techniques.

Unit II: (Hours -08)
Investigating Web Attacks: Indication of Web Attacks, Types of Web Attacks, Overview of WebLogs, Investigating Web Attacks, FTP Servers IIS Logs, Apache Logs Windows based Servers, Intrusion Detection, Tools for Locating IP Addresses,

Unit III: (Hours- 08)
Router Forensics: Introduction, Function of a Router, Router Vulnerabilities, Attacks, Router Forensics versus Traditional Forensics, Investigating Router Attacks etc., Investigating DoS Attacks:
Introduction, Indication of DoS Attacks, Types of DoS Attacks, DDos Attacks, Dos Attacks Modes, Techniques to detect Dos Attacks, Investigating Dos Attacks.

Unit IV: (Hours – 08)
Investigating Internet Crime: Introduction, Internet Crime, Internet Forensics, Goals of Investigation, Steps for Investigating Internet Crimes, Tracking E-Mails and Investigating E- Mails Crime: Introduction, E-Mail Systems, E-Mail Crimes, Identify thefts, Chain E-Mails, Phishing, E-Mail Spoofing, Investigating E-Mails Crimes and Violations, Using Specialized E- Mails Forensics Tools.

Unit V: (Hours – 08)
Investigating Corporate Espionage: Introduction, Motive behind Spying, Insider/Outsider threat, Techniques of Spying, Defence against Corporate Spying, Steps to prevent Corporate Espionage,Investigating Trademark and Copyright Infringement: Introduction, Trademarks, Trademarks Infringement, Copyrights, Patent, Domain Name Infringement, Intellectual Property, Digital Rights Management(DRM), Indian Law for Trademarks and Copyrights.

Unit VI: (Hours – 08)
Investigating Sexual Harassment Incidents: Introduction, Types of Sexual Harassments and its Consequences, Statistics, Do's and Don't, Stalking, Responsibilities of Supervisors and Employees, Complaint Procedure, Investigation process, Sexual Harassment Policy, Preventive Steps, Indian Laws, Investigating Child Pornography: Introduction, Peoples motives behind child pornography, Peoples involved, Role of Internet in Child Pornography, Effects of Child Pornography on Children, Measures to prevent dissemination, Challenges in controlling child pornography, Precautions and steps to investigate child pornography, Sources of Digital Evidence etc.

Text Book:
EC Council Press, Course Technology, Cengage Learning, 2010, "Investigating Network Intrusions and Cybercrime"

Reference Books:
1. Sagar R. Kothari, "Cyber Crime Investigations: An Introduction"
2. Kuldeep Sharma and Reema Sharma, "Cyber Crime Investigation and Cyber Forensics: A Case Study Approach"
3. Bruce Middleton and Karen A. Forcht, "Investigating Cyber Crime: A Guide for the LegalProfessional"
4. Brett Shavers, "Cybercrime Investigation Case Studies: An Excerpt from Placing the SuspectBehind the Keyboard"
5. Nagarathna A., Pradeep K. & Vidya V, "Cyber Crime and Digital Evidence: Cases andMaterials".

1PGDCY 04 Lab-1: Based on Introduction to Cyber Security and Cyber Crime & Investigation Procedures: Minimum Ten experiments / programming assignments must be completed based on the respective syllabus (1PGDCY 02 and 1PGDCY 03) covering each of the units.

1PGDCY 05 PROJECT / SEMINAR – I:

Every student has to submit seminar report and deliver a seminar on advance state-of the-art topics.

Seminar Course Outcomes:
After completion of the Seminar, the students would be able to:
1. Study research papers published in peer-reviewed journals for understanding of a new field, inthe absence of a textbook, to summarise and review them.
2. Identify promising new directions of various cutting-edge technologies
3. Impart skills in preparing detailed seminar report
4. Communicate effectively by making an oral presentation before an evaluation committee

Project Course Outcome:
After completion of the course the students would be able to:
1. Demonstrate a sound technical knowledge of their selected project topic/problem.
2. Undertake problem identification, formulation, objectives and solution.
3. Design/develop the solution to a problem
4. Inculcate the ability to synthesize the results of the detailed analytical studies conducted, lay down validity and design criteria, interpret the result for application to the problem, develop the concept and detailed design solution and to effectively communicate the Project Report rationale
5. Demonstrate the knowledge, skills and attitudes of a professional.

Project work: A project work in the 1st & 2nd semester has been included in the curriculum to enable the students to get familiar with the practices and procedures being followed in the industries and provide an opportunity to work on some live projects in the industry. A project report should be submitted in three copies.

● The students would develop their project individually and get the topic approved by the head/ director/principal of the college. For the purpose of approval, they have to submit their project titles and proposals with the name of internal guides to the head/ director/principal of the college within 45 days of the commencement of the semester. The concerned college/institute shall submit the project titles along with the proposals and name of the internal guides to the university for due approval. In case, if the student proposal is rejected, the revised proposal, is
required to submit and get it sanctioned within next seven days. Failing to do this, He/she will not be qualified for this subject/course.

● The students have to report to the guide for at least three times during the project lifespan with the progress report duly signed by the internal guide. Moreover, they have to submit the progress reports with the final project report at the time of external examination.

● The external examiners appointed by the University shall award the marks on the basis of the Presentation, Demonstration, Viva-Voce, and on the basis of Project Report.

1PGDCY 06 INTERNSHIP /APPRENTICESHIP/FIELD WORK / WORK EXPERIENCE:
Students are required to undertake mandatory Internship /Apprenticeship/Field Work / Work Experience (During vacation of Semester I) for duration of 60 hours in including but not limitedto cyber cell, certified forensic examiners, cyber law practitioners, cyber forensic laboratory, etc. during vacation of Semester I. This will carry 2 Credits for learning of 60 hours. Its credits and grades will be reflected in final semester II credit grade report.

2PGDCY 01 CYBER LAW – II (L-4, T-0, P-0, C-4)

Course Pre-requisite: Introduction to Computers, Cyber Law – I, Cyber Security

Course Objectives: Throughout the course, students will be expected to demonstrate their understanding ofIntellectual Property, Intellectual Property Rights and its related Laws by being able to do eachof the following:

1. To understand various key paradigms for Intellectual Property.
2. To familiarize with the Intellectual Property Rights (IPR).
3. To understand IPR and its related Laws

Course Outcomes (Expected Outcome): After Successful completion of this course, the studentwould be able to:

1. Understand fundamentals of Intellectual Property
2. Describe Impact of IT Act and Forms of Intellectual Property
3. Classify Intellectual Property in Indian Perspective
4. Understand Role of Intellectual Property Rights and its related Laws.

Unit I: Intellectual Property and Intellectual Property Rights (IPRs): (Hours-09)

An Over View of Intellectual Property, Industrial Property and IPRs, Philosophical Theories on Intellectual Property, International and National Concern for IPRs, Emerging Dimensions of IPR Regime

Unit II: Law on Copyright: (Hours-09)
Copyright in General, Registration, publication, and licence etc. including a few special rights, Infringement of Copyright, Enforcement of Copyright, International Copyright and Case Law.

Unit III: Law on Patents: (Hours-09)

Patents in General, Obtaining patent and Patentee, Transfer, Surrender, Revocation and Restoration of Patent, Infringement and Enforcement, Important Issues, Case Laws on Patents.

Unit IV: Law on Trademarks: (Hours-09)
Trademarks in General, Registration, rights, assignment and transmission of trademark, Infringement and Passing off Action in Trademark, Remedies and Authorities, Case law on Trademarks.

Unit V: Law on Designs: (Hours-06)
Designs in General, Registration, Rights, Infringement and Remedies, Case Law on Designs.

Unit VI: Law of Geographical Indication and Traditional Knowledge (Hours-06)

Geographical Indications in General, Registration, Infringement and Remedies of GeographicalIndications, Protection of Traditional Knowledge.

Text Book: B.L. Wadehra, " Law relating to Intellectual Property**".**

Reference Books:

1. S.K. Singh "Intellectual Property Rights Laws"
2. M.K. Bhadari "Law Relating to Intellectual Property Rights"
3. T. Ramappa "Intellectual Property"

2PGDCY 02 SYSTEM AND SOFTWARE SECURITY (L-4, T-0, P-0, C-4)

Course Pre-requisite: Computer Fundamentals, Basics of Cyber Security, Cyber Law

Course Objectives: Throughout the course, students will be expected to demonstrate theirunderstanding of System and Software Security by being able to do each of the following:

- To provide an in-depth study of concepts and threats in computer security.
- To provide knowledge of common vulnerabilities, attack mechanisms and methodsagainst computer and information system
- To familiarize security issues at various levels such as operating systems and databases.
- To provide the study of vulnerability issues and its counter measures at advancedapplication such as networks and Clouds

Course Outcomes (Expected Outcome): On completion of the course, the students would beable to:

1. Co-relate malicious and non-malicious attacks.
2. Outline web common vulnerabilities, attack mechanisms and methods against computerand information systems.
3. Apply relevant methods for security modeling and analysis of Operating System.
4. Investigate a secure network by monitoring and analyzing the nature of attacks.
5. Explain cryptography, intrusion detection and firewall system
6. Implement different security solutions at various levels such as operating systems,databases and clouds.

Unit I: (Hours: 08)

Programs and Programming: Unintentional (Non malicious) Programming: Buffer Overflow, Incomplete Mediation, Time-of-Check to Time-of Use, Undocumented Access Point, Off-by- One Error, Integer Overflow, Unterminated Null-Terminated String, Parameter Length, Type andNumber, Unsafe Utility Program, Race Condition. Malicious Code: Malware: Viruses, Trojan Horses, and Worms, Technical Details: Malicious Code. Countermeasures: Countermeasures for Users, Countermeasures for Developers, Countermeasure Specifically for Security, Countermeasures that Don't Work.

Unit II: (Hours: 08)

The Web: Browser Attacks: Browser Attack Types, How Browser Attacks Succeed: Failed Identification and Authentication. Web Attacks Targeting Users: False or Misleading Content, Malicious Web Content, Protecting Against Malicious Web Pages. Obtaining User or Website Data: Code Within Data, Website Data: A User's Problem, Too Foiling Data Attacks. Email Attacks: Fake Email, Fake Email Messages as Spam, Fake (Inaccurate) Email Header Data, Phishing, Protecting Against Email Attacks.

Unit III: (Hours :08)

Operating System: Security in Operating Systems: Operating System Structure, Security Features of Ordinary Operating Systems, Protected Objects, Operating System Tools to Implement Security Functions. Security in the Design of Operating Systems: Simplicity ofDesign, Layered Design, Kernelized Design, Reference Monitor, Correctness and Completeness, Secure Design Principles, Trusted Systems, Trusted System Functions, The Results of Trusted Systems Research Rootkit: Phone Rootkit, Rootkit Evades Detection, Rootkit Operates Unchecked, Sony XCP Rootkit, TDSS Rootkits, Other Rootkits.

Unit IV: (Hours: 08)

Networks: Network Concepts, Threats to Network Communications: Interception: Eavesdropping and Wiretapping, Modification, Fabrication: Data Corruption Interruption: Loss of Service, Port Scanning, Vulnerability. Wireless Network Security: Vulnerabilities in Wireless Networks, Failed Countermeasure: WEP (Wired Equivalent Privacy), Stronger Protocol Suite: WPA (Wi-Fi Protected Access) Denial of Service: Network Flooding Caused by MaliciousCode, Network Flooding by Resource Exhaustion, Denial of Service by Addressing Failures, Traffic Redirection, DNS Attacks, Exploiting Known Vulnerabilities, Physical Disconnection. Distributed Denial-of-Service: Scripted Denial-of-Service Attacks, Bots, Botnets, Malicious Autonomous Mobile Agents, Autonomous Mobile Protective Agents.

Unit V: (Hours: 08)

Cryptography in Network Security Browser Encryption, Onion Routing, IP Security Protocol Suite (IPsec), Virtual Private Networks, System Architecture. Firewalls: Firewall, Design of Firewalls, Types of Firewalls, Personal Firewalls Comparison of Firewall Types, Example Firewall Configurations. Intrusion Detection and Prevention Systems: Types of IDSs, Other Intrusion Detection Technology, Intrusion Prevention Systems, Intrusion Response, Goals for Intrusion Detection Systems, IDS Strengths and Limitations.

Unit VI: (Hours:08)

Database: Security Requirements of Databases: Integrity of the Database, Element Integrity, Auditability, Access Control, User Authentication, Availability,Integrity / Confidentiality / Availability. Reliability and Integrity: Protection Features from the Operating System, Two-Phase Update Redundancy/Internal Consistency, Recovery, Concurrency/Consistency. Database Disclosure: Sensitive Data, Types of Disclosures, Preventing Disclosure: Data Suppression and Modification, Security Versus Precision DataMining and Big Data: Data Mining, Big Data. Cloud Computing: Cloud Computing Concepts: Service Models, Deployment Models. Risk Analysis: Cloud Provider Assessment, Switching Cloud Providers, Cloud as a Security Control. Cloud Security Tools and Techniques: Data Protection in the Cloud, Cloud Application Security, Logging and Incident Response. Cloud Identity Management: Security Assertion Markup Language OAuth: OAuth for Authentication. Securing IaaS: Public IaaS Versus Private Network Security.

Text Book:

Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Fifth Edition, Prentice Hall, 2015

Reference Books:

1. Computer Security: Principles and Practice, William Stallings and Lawrie Brown, ThirdEdition, Pearson Prentice Hall.
2. Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing Achyut S.Godbole, Tata Mc Graw-Hill Education, 2013.
3. Cryptography and Network Security Principles and Practices, William Stallings, Seventh Edition, Pearson.
4. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, AddisonWesley, 2011.

2PGDCY 03 DIGITAL FORENSICS (L-4, T-0, C-4)

Course Pre-requisite: Cyber Law, Introduction to Cyber Security, Cyber Crimes & Investigation Procedures.

Course Objectives: Throughout the course, students will be expected to demonstrate theirunderstanding of Digital Forensics by being able to do each of the following:

- To understand the basic digital forensics and techniques for conducting theforensic examination on different digital devices.
- To understand how to examine digital evidences such as the data acquisition,identification analysis.
- To understand the basics of mobile phone forensics.
- To understand the network based cyber security intrusion detection.
- To know the various forensics tool.

Course Outcomes (Expected Outcome): On completion of the course, the students would be able to:

1. Describe Digital Forensics and its related preparation
2. Outline Data Acquisition tools
3. Use knowledge to improve crime investigations.
4. Examine Digital Forensic and its validation
5. Assess role of email and social media in investigations
6. Analyze Cloud Forensics.

Unit I: (Hours: 08)
Introduction: An Overview of Digital Forensics, Preparing for Digital Investigations, PreparingA Digital Forensics Investigations, Procedure for Private Sector High-Tech investigations, understanding data recovery work station and software, conducting and investigations.

Unit II: (Hours: 08)
Data Acquisition: Understanding storage formats for digital evidence, determining the bestacquisition method, Contingency planning for Image acquisition, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools.

Unit III: (Hours: 08)
Processing Crime and Incident Scenes: Identifying Digital Evidence, Collection Evidence in Private Sector Scenes, Processing Law Enforcement Crime Scenes, Preparing for a search,Securing a Digital Incident or Crime Scene, Seizing Digital Evidence at the scene, Storing a Digital Evidence, Obtaining a Digital Hash,

Unit IV: (Hours: 08)
Digital Forensic Analysis and Validation: Data to collect and analyze, Validating Forensic data, Addressing data hiding techniques, Virtual Machine Forensics, Live Acquisition and Network Forensics

Unit V: (Hours:08)
Email and Social Media Investigations: Role of Email in investigations, Roles of Client and server in Email, Investigating Emails Crimes and Violations, Email Servers, Specialize Email Forensic Tools, Digital Forensics to Social Media Communications. Mobile Device Forensicsand Internet of Anything: Mobile Device Forensics, Acquisitions procedure for Mobile Devices, Forensics in Internet of Anything.

Unit VI: (Hours: 08)
Cloud Forensics: Cloud Computing, Legal Challenges in Cloud Forensics, Technical Challenges in Cloud Forensics, Acquisitions in the cloud, Conducting a cloud investigation, Tools for Cloud Forensics. Digital Forensics Tools: Evaluating Digital Forensics Tools Needs, Software and Hardware Tools, Validating and Testing Software.

Text Book:
Nelson, B, Phillips, A, Stuart, C., “Guide to Computer Forensics and Investigations”, 6th edition,Cengage Learning.

Reference Books:

1. Warren G. Kruse II and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.
2. Davidoff, S. and Ham, J., Network Forensics Tracking Hackers through Cyberspace,Prentice Hall, 2012.
3. Michael G. Solomon, K Rudolph, Ed Tittel, Broom N., and Barrett D., ComputerForensics Jump Start, Willey Publishing, Inc., 2011.
4. Marcella, Albert J., Cyber forensics: A field manual for collecting, examining andpreserving evidence of computer crimes, New York, Auerbach publications, 2008.
5. Davidoff, Sherri, Network forensics: Tracking hackers through cyberspace, Pearsoneducation India private limited, 2017.
6. John Sammons, The Basics of Digital Forensics, Elsevier, 1st Edition, 2015.

2PGDCY 04 Lab-2: Based on Systems and Software Security, Digital Forensics: Minimum Ten experiments / programming assignments must be completed based on the respective syllabus (2PGDCY 02 and 2PGDCY 03) covering each of the units.

2PGDCY 05 PROJECT / SEMINAR – II:

Every student has to submit seminar report and deliver a seminar on advance state-of the-arttopics.

Seminar Course Outcomes:

After completion of the Seminar, the students would be able to:

1. Study research papers published in peer-reviewed journals for understanding of a new field, inthe absence of a a textbook, to summarise and review them.
2. Identify promising new directions of various cutting-edge technologies
3. Impart skills in preparing detailed seminar report
4. Communicate effectively by making an oral presentation before an evaluation committee

Project Course Outcome:

After completion of the course the students would be able to:

1. Demonstrate a sound technical knowledge of their selected project topic/problem.
2. Undertake problem identification, formulation, objectives and solution.
3. Design/develop the solution to a problem
4. Inculcate the ability to synthesize the results of the detailed analytical studies conducted, lay down validity and design criteria, interpret the result for application to the problem, develop the concept and detailed design solution and to effectively communicate the Project Report rationale.
5. Demonstrate the knowledge, skills and attitudes of a professional.

Project work: A project work in the 1st & 2nd semester has been included in the curriculum to enable the students to get familiar with the practices and procedures being followed in the industries and provide an opportunity to work on some live projects in the industry. A project report should be submitted in three copies.

- The students would develop their project individually and get the topic approved by the head/ director/principal of the college. For the purpose of approval, they have to submit their project titles and proposals with the name of internal guides to the head/ director/principal of the college within 45 days of the commencement of the semester. The concerned college/institute shall submit the project titles along with the proposals and name of the internal guides to the university for due approval. In case, if the student proposal is rejected, the revised proposal, is required to submit and get it sanctioned within next seven days. Failing to do this, He/she willnot be qualified for this subject/course.
- The students have to report to the guide for at least three times during the project lifespan with the progress report duly signed by the internal guide. Moreover, they have to submit the progress reports with the final project report at the time of external examination.
- The external examiners appointed by the University shall award the marks on the basis of the Presentation, Demonstration, Viva-Voce, and on the basis of Project Report.

****