Syllabus for P.G. Diploma in Cyber Law and Information Technology

Paper – I: Basic of computer and Cyber Security

Paper – II: Information Technology Law (Cyber Law)

Paper – III: Cyber crime and investigation procedures

Paper – IV: Practical Training / Field work

Paper – I

Basic of computer and Cyber Security

1. History of Computers, Areas of Application
2. Computers and its components, Application Software and System Software
3. Introduction to Operating System
4. Basics of Networks and internet, Types of Network, Definition of Cyber Security
5. Search Engines, E –mails and WWW; Internetworking Devices, Internet Service provider, IP Address, Working of Email system, Domain Name System, Blogs, Peer to peer sharing
6. Cryptography, type, goals , PKI
7. Digital signatures and electronic signatures, Electronic Payment System and Taxation.
8. Computer & Cyber Security:
   (a) Types of Attacks,
   (b) Network Security
   (c) Overview of Security threats,
   (d) Hacking Techniques,
   (e) Password cracking
   (f) Insecure Network connections,
   (g) Malicious code
   (h) Concept of Fire wall Security
9. Email security: web authentication, SSL and SET
10. Database Security
11. Operating System Security
12. E – commerce & M – commerce System Security
13. Advance Computers, Network & Mobile Security Techniques

Paper – II

Information Technology Law

(Cyber Law)

1. Evolution of the IT Act, Genesis and Necessity
2. Salient features of the IT Act, 2000, various authorities under IT Act and their powers. ; Penalties & Offences, amendments.
3. Impact on other related Acts (Amendments) :
   (a) Amendments to Indian Penal Code.
   (b) Amendments to Indian Evidence Act.
   (c) Amendments to Bankers Book Evidence Act.
   (d) Amendments to Reserve Bank of India Act.
4. Cyber Space Jurisdiction
   (a) Jurisdiction issues under IT Act, 2000.
   (b) Traditional principals of Jurisdiction
   (c) Extra terrestrial Jurisdiction
   (d) Case Laws on Cyber Space Jurisdiction
5. E – commerce and Laws in India
   (a) Digital / Electronic Signature in Indian Laws
   (b) E – Commerce; Issues and provisions in Indian Law
   (c) E – Governance; concept and practicality in India
   (d) E – Taxation issues in Cyberspace
   (e) E – Contracts and its validity in India
   (f) Cyber Tribunal & Appellate Tribunal
   (g) Cyber Regulations
6. Intellectual Property Rights, Domain Names and Trademark Disputes
   (a) Concept of Trademarks / in Internet Era
   (b) Cyber Squatting
   (c) Reverse Hijacking
   (d) Jurisdiction in Trademark Disputes
   (e) Copyright in the Digital Medium
   (f) Copyright in Computer Programmes
   (g) Copyright and WIPO Treaties

(h) Concept of Patent Right

(i) Relevant Provisions of Patent Act 1970

7. Sensitive Personal Data or Information (SPDI) in Cyber Law
   (a) SPDI Definition and Reasonable Security Practices in India
   (b) Reasonable Security Practices – International perspective
8. Cloud Computing & Law
9. Cyber Law : International Perspective
   (a) EDI: Concept and legal Issues.
   (b) UNCITRAL Model Law.
   (c) Electronic Signature Law's of Major Countries
   (d) Cryptography Laws
   (e) Cyber Law's of Major Countries
   (f) EU Convention on Cyber Crime

Paper – III

Cyber crime and investigation procedures

1. Cyber Forensic and Computer Crimes and types. Crimes targeting Computers: Definition of Cyber Crime & Computer related Crimes, Classification & Differentiation between traditional crime and cyber crimes.
   (a) Data Theft
   (b) Hacking
   (c) Spreading Virus & Worms
   (d) Phishing
   (e) Cyber Stalking / Bullying
   (f) Identity Theft & Impersonation
   (g) Credit card & Online Banking Frauds
   (h) Obscenity, Pornography & Child Pornography
   (i) Cyber Defamation, Defacement,
   (j) Illegal online selling & Gambling
   (k) Denial of Service Attacks
   (l) Cyber terrorism
   (m) Software Piracy & illegal downloading
2. Reasons for Cyber Crimes.

3. Cyber Criminal Mode and Manner of Committing Cyber Crime
4. Prevention of Cyber Crimes & Frauds Critical analysis & loop holes of The IT Act, 2000
5. Cyber Crimes: Freedom of speech in cyber space & human right issues
6. Investigation of Cyber Crimes
7. Investigation of malicious applications
8. Agencies for investigation in India, their powers and their constitution as per Indian Laws
9. Procedures followed by First Responders;
10. Search and Seizure Procedures of Digital Evidence
11. Securing the Scene , Documenting the Scene, Evidence Collection and Transportation
    (a) Data Acquisition
    (b) Data Analysis
    (c) Reporting
12. Digital Forensics
    (a) Computer Forensics
    (b) Mobile Forensics
    (c) Forensic Tools
    (d) Anti – Forensics
13. Electronic / Digital Evidence laws & cases Laws
14. International Organizations and Their Roles
    (a) ICANN
    (b) URDP
    (c) WTO and TRIPS
    (d) Interpol & Europol
    (e) Impact of Cyber warfare on Privacy Identity
    (f) Net Neutrality and EU Electronic communication Regulatory framework
    (g) WCAG
    (h) Social Networking sites Vis – a – Vis Human Right
15. Case Laws : Indian & International Cases

Paper – IV

Practical Training / Project Work

The project report submitted by the student will be evaluated jointly by the internal and external examiners during the practical examination. The distribution of marks will be as follows:

(a) Dissertation	:	40 Marks
(b) Report of field work & Presentation	:	40 Marks
(c) Viva – Voice	:	10 Marks
(d) Attendance	:	10 Marks

RECOMMENDED BOOKS:

1. Cyber Law & Cyber Crimes By Advocat Prashant Mali; Snow White publications, Mumbai
2. Cyber Law in India by Farooq Ahmad; Pioneer Books
3. Information Technology Law and Practice by Vakul Sharma; Universal Law Publishing Co. Pvt. Ltd.
4. The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi
5. Guide to Cyber and E – Commerce Laws by P.M. Bukshi and R.K. Suri; Bharat Law House, New Delhi
6. Guide to Cyber Laws by Rodney D. Ryder; Wadhwa and Company, Nagpur
7. The Information Technology Act, 2000; Bare Act – Professional Book Publishers, New Delhi
8. Computer Forensics: Principals and Practices by Linda Volonino, Reynaldo Anzaldua and Jana Godwin; Pearson Prentice – Hall 2007
9. First Responder's Guide to Computer Forensics by Richard Nolan rt al; Carnegi Mellon, 2005.
10. Digital Evidence and Computer Crime, 2nd Ed. By Eoghan Casey; Academic Press, 2004.
11. The Regulation of Cyberspace by Andrew Murray, 2006; Rutledge – Cavendish.
12. Scene of the Cybercrime: Computer Forensics Handbook by Syngress.
13. Security and Incident Response by Keith J. Jones, Richard Bejtloich and Curtis W. Rose

14. List of Websites for more information is available on:
    Http://www.garykessler.net.library/ forensicsurl.html
15. Introduction to Forensic Science in Crime Investigation by Dr. (Smt) Rukmani Krishnamurthy.