

FACULTY OF LAWS

SYLLABUS

FOR

P.G. DIPLOMA IN CYBER LAW & INFORMATION SECURITY

**(Semester: I-II)
SESSION: 2019-20**



**GURU NANAK DEV UNIVERSITY
AMRITSAR**

- Note:** (i) Copy rights are reserved.
Nobody is allowed to print it in any form.
Defaulters will be prosecuted.
- (ii) Subject to change in the syllabi at any time.
Please visit the University website time to time.

SCHEME

Semester-I		
Course No.	Title of the course	Marks
LPL101	CYBER WORLD AND CYBER ETHICS	100
LPL102	CYBER CRIMES	100
LPL103	INFORMATION SECURITY, CRIME AND INVESTIGATION	100

Semester-II		
Course No.	Title of the course	Marks
LPL104	INTERNATIONAL TREATIES, IPR & CYBER WORLD	100
PL105	ELECTRONIC COMMERCE	100
LPL106	COMPUTER SECURITY, AUDIT AND ASSURANCE	100

LPL 101: CYBER WORLD AND CYBER ETHICS**Time: 3 Hrs.****Total Marks: 100****Instructions for the Paper Setters:-**

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION A

Computer and its role in day to day life
Advantages and Disadvantages of Internet Technology
Increasing digitalization
E-Governance and E-Records
Cyber Ethics
Online Plagiarism

SECTION B**Information Technology Act 2000**

Need, Aims, Objectives and Applications [Section 1]
Definitions [Section 2]
Attribution of records
Certifying Authority [Sections 30-34]
Cyber contraventions and penalty [Sections 43-45]
Offences and extra territorial jurisdiction [Sections 65-77]
Intermediary not liable in certain cases [Section 2 (w), 79]
Investigation and procedure of search and seizure [Sections 78 & 80]
Amendments under IT Act 2008.

SECTION C

International Legal Regime relating to Cyber Crimes

UNICTRAL Model law on Electronic Commerce

European Convention on Cyber Crimes

Hague Convention on Jurisdiction and Foreign Judgments: Jurisdiction Agreement

SECTION D

Online Vulnerability of certain sections such as children, young adults, senior citizens,

Minorities, Backward classes and women

Regulating the functioning of Social Sites

Online Hate Crimes

Scope of Cyber laws

Jurisdictional Issues

References:

1. Pavan Duggal: Cyber Law- The Indian Perspective, Saakshar Publications, New Delhi, 2002; Second Edition
2. Vakul Sharma: Information Technology: Law and Practice, Universal Law Publishing Co., New Delhi, 2011;
3. Harish Chander: PHI, 2012;
4. Nandan Kamath: Law Relating to Computers, Internet, and E-Commerce: A Guide to Cyber Laws and the Information Technology Act 2000 with Rules and Notifications, Second Edition, Universal Law Publishing Co., New Delhi, 2000

LPL102: CYBER CRIMES**Time: 3 Hrs.****Total Marks: 100****Instructions for the Paper Setters:-**

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION A**Cyber Crimes:**

Meaning Nature & Classification;

Distinction between Conventional Crime and Cyber Crimes;

Major kinds of Cyber Crimes

The Indian Penal Law and Cyber Crimes

Fraud

Hacking

Mischief

Trespass

Defamation

Stalking

Spamming

SECTION B

Domestic Legal Regime relating to Cyber Crimes

IT Amendment Act, 2008

Suggested Amendments

Relevant provisions under Indian Evidence Act, Pornography Act etc.

SECTION C**Jurisdictional Issues:**

Definition

Jurisdiction to prescribe/Legislative Jurisdiction;

Jurisdiction to adjudicate to enforce;

Cyber Jurisdiction in Civil, Criminal & International Cases.

Laws & Acts:

Unictral Model Law,

Information Technology Act, 2000 including Relevant Rules and Notifications,

SECTION D**Judgments:**

CBI v. Abhishek Verma, (2009)6SCC300

Bhavesh Jayanti Lakhani v. State of Maharashtra, (2010)1 SCC (Cri.)47

Director General of Doordarshan v. Anand Patwardhan, (2006)8SCC433

Shreya Singhal v. Union of India, AIR 2015SC 1523

Ranjit Udeshi v. State of Maharashtra, AIR 1965 SC 881

Cellular Operators Association of India v. Union of India, (2003) 3 SCC186

Ajay Goswami v. Union of India, (2007) 1 SCC 170

Nasscom v. Ajay Sood & others, (2005)DLT596

Avnish Bajaj v. State (N.C.T.) of Delhi. (2005)DLT427

Reference Material:

1. Pavan Duggal: Cyber Law- The Indian Perspective, Saakshar Publications, New Delhi, 2002. Second Edition
2. Vakul Sharma: Information Technology: Law and Practice, Universal Law Publishing Co., New Delhi, 2011
3. Harish Chander: PHI, 2012
4. Nandan Kamath: Law Relating to Computers, Internet, and E-Commerce: A Guide to Cyber Laws and the Information Technology Act 2000 with Rules and Notifications, Second Edition, Universal Law Publishing Co., New Delhi, 2000

LPL103: INFORMATION SECURITY, CRIME AND INVESTIGATION**Time: 3 Hrs.****Total Marks: 100****Instructions for the Paper Setters:-**

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION A

The State of threats against computers, and networked systems,
Overview of computer Security,
Vulnerability assessment, managing firewalls and VPNs,
Overview of Intrusion Detection and Intrusion prevention Network and host-based IDS
Classes of attackers, Kids/ hackers/ sophisticated groups, automated: Drones, Worms and Viruses

SECTION B

Information security risk analysis fundamentals Importance of physical security and Biometrics controls for protecting information systems assets,
Security considerations for the mobile work force,
Network security perspectives, networking and digital communications, security of wireless networks.

SECTION C

Security models and frameworks and standards through introduction to the ISO 27001, SSECMM (systems security engineering – capability maturity model), COBIT (Control Objectives for Information and related technologies) and the Sarbanes-Oxley Act (SOX) and SAS 70 (statement on auditing standards),
Privacy Fundamentals, business practices, impact on data privacy,
Technological impact on data privacy, privacy issues in web services and applications based on web services.

SECTION D

Internet/Computer Demographics: Computer/network user statistics;

Computer crime statistics,

Types of Computer and Internet Crime: Types of crimes involving computers;

Computer crimes; Network crimes; Criminals, hackers, and crackers

Investigations: The investigation life cycle; Legal methods to obtain the computer;

Jurisdictions and agencies; Internet investigations (e-mail, IRC, chat rooms, etc.);

IP addresses and domain names; Investigative methods, Digital Evidence

Evidence Collection: Working with ISPs and telephone companies; Examining computer,

Server, and network logs; Anonymous services.

Text/ References Books:

1. Information Systems Security Management by Nina S. Godbole (Wiley India Pvt.Ltd.)
2. Security Engineering by Ross Anderson
3. Information Security Management Handbook by Harold Tpton & Micki Krause
(Auerbach Publications)
4. Network Security Essentials: Applications and Standards W. Stallings (Pearson
Education)
5. Security Planning & Disaster Recovery by Eric Maiwald and William Sieglein (Tata
McGraw-Hill)
6. M. Erbschloe, J. R. Vacca: Information Warfare: How to Survive Cyber Attacks
(McGraw-Hill Prof. 2001.)
7. Jones, G. L. Kovacich, and P. G. Luzwick: Global Information Warfare: How Business,
Governments, and Others Achieve Objectives and Attain Competitive Advantages (CRC
Press, 2002.)
8. D. Denning: Information Warfare and Security (Addison Wesley) 1998.

LPL 104: INTERNATIONAL TREATIES, IPR & CYBER WORLD**Time: 3 Hrs.****Total Marks: 100****Instructions for the Paper Setters:-**

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION A**Introduction:**

Introduction to Intellectual Property Rights

GATT & WTO,

WIPO,

TRIPS,

Berne Convention,

Universal Copyright Convention,

Copyright Treaty (WCT),

Copyright Act 1957,

Trades Marks Act, 1999, Definition, Breach and remedies.

SECTION B

Data Protection: Meaning

Principles of Data Protection

Jurisdictional issues

Retention of e- records

Transnational Data Flow and International Controls

Uniform Domain Name Dispute Resolution Policy.

SECTION C**International Treaties:**

PCT,

PLT,

SPLT,

Washington Treaty

SECTION D**Patents:**

Indian Patent Act, Definitions breach and remedies,

Application of Patents to information Technology;

Patents for computer software,

Patents for electronic commerce,

Patent and Patentability criteria in India, US, EPC, Japan, China, Singapore etc.

Various national and International Patent classifications

LPL 105 ELECTRONIC COMMERCE**Time: 3 Hrs.****Total Marks: 100****Instructions for the Paper Setters:-**

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION A

Meaning, Scope and Changing Dimensions

E-Commerce v. Traditional Commerce

E-Commerce and E-business Models(B2C, B2B, C2C, C2B)

Advantages and Disadvantages

Global Trends

SECTION B

Online Contracts-Relevant provisions of the Indian Contract Act, 1872 and IT Act, 2000.

Issues relating to Jurisdiction, Online Dispute Resolution, including the Role of WTO

Issues relating to Access

Issues relating to Infrastructure

Digital Divide

Privacy

Security

SECTION C

1. UNICTRAL Model law on E-Commerce
2. Threats to E-Commerce
3. Inaccurate Management
4. Price Manipulation
5. Spam
6. Malicious code threats
7. Hactivism
8. Wi-fi Eavesdropping

SECTION D

Disintermediation and Re-intermediation,

Bitcoins

Internet and Mobile Banking,

Online Payment Gateways,

Electronic money/Truncated Cheque/Electronic Cheque

Regulating E-transactions including Role of RBI

Countering Cyber Attacks

Secure electronic transactions

Encryption

Digital Certificates

Security Audit

References:

1. Rajaraman, "Introduction to Information technology", Prentice Hall of India, Ed., 2005.
2. Edwards, et al., "The essence of Information Systems, Prentice Hall of India, 2nd Ed., 2005.
3. Murdick, Ross & Claggett, "Information Systems for Modern Management", Prentice Hall of India, 3rd Ed., 2005.

LPL 106: COMPUTER SECURITY, AUDIT AND ASSURANCE**Time: 3 Hrs.****Total Marks: 100****Instructions for the Paper Setters:-**

Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION A

Introduction to computer based systems and their Security, Policy standards and Organization, Information Classification and Security awareness.

Information System Audit and Assurance - An Overview, Determination of policy and the degree of assurance required from controls,

Information Security Management System (ISMS),

Audit and review of ISMS Internal Control and Information System Audit information

Security Governance and Assurance and Audit Security Controls,

Systems Assurance and Control (SAC), Systems Audit ability and Control (SAC) reports,

Control Objectives for Information and Related Technologies

SECTION B

Attack and Threat Analysis, various types of Attacks and Threats and their Analysis on Security,

Security Management techniques,

Infrastructure assessments, System assessments, Business case assessments for improvements.

Study of various tools and techniques available for Security risk analysis

Security Controls, Physical Security,

Virtual Private Networks (VPNs), IP sec, Access Controls,

Identification and Authentication Techniques, Managed Firewalls, Data Monitoring Software,

Email Security

Cryptology.

SECTION C

Security Policies and Procedures,

An investigation into the types of policies and procedures

How to formulate your IT Security Policy, IT Policy standards,

Creating, implementing, and managing controls and monitoring mechanisms, as well as other important security policies and procedures.

SECTION D

IT Security Audits, Systematic technical assessments , personal interviewing, vulnerability scanning, examining operating system settings,

Analysis of network shares, review of firewall management, physical security, penetration test techniques, reviewing audit logs, look at encryption used, and view documentation from any changes to systems or software.

Text/ References:

1. Fischer & Jordan, "Security Analysis and Portfolio Management", 6th Ed., Prentice Hall of India, Ed., 2005.
2. Rajaraman, "Introduction to Information technology", Prentice Hall of India, Ed., 2005.
3. Edwards, et al., "The essence of Information Systems, Prentice Hall of India, 2nd Ed., 2005.
4. Murdick, Ross & Claggett, "Information Systems for Modern Management", Prentice Hall of India, 3rd Ed., 2005.
5. A. Blyth and G. L. Kovacich, "Information Assurance", Springer, 2005.