PG Diploma in Cyber Crime and Law 2019-2020

(1-year program)

**Salient Features**

1. With the advancement of Information Communication Technology and the good amount of knowledge shared through internet has encouraged the techno savoy young generation to indulge in cyber-crime. This Cyber Space and its IT infrastructure are very much vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. As the cyber-crime is borderless and very delegate to handle, it needs special tools and technology in-order to prevent different types of Cyber-attacks and gather digital evidence without any kind of damage. For the admissibility of the evidence in the court, the evidence must be preserved and handled to ensure that it hasn’t been changed. Apart from this the rise and evolution of social media has changed the definition of communication and social interaction.

2. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence there is a need for cyber laws. Cyber law touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. Hence, this course will allow the participants to get a vivid knowledge of how crime is committed in the cyber world, the manner in which these crimes are being investigated including evidence collection and examination of the evidences and the laws pertaining to such crimes, handling evidences, maintaining the chain of custody and presenting the facts and findings in the court.
**Course Objectives**

The course has been designed keeping in mind the following objectives:

1. This course will look at the emerging legal, policy and regulatory issues pertaining to cyberspace and cybercrimes.

2. To cover all the topics from fundamental knowledge of Information Technology and Computer Architecture so that the participant can use to understand various aspects of working of a computer.

3. To identify the emerging Cyberlaws, Cybercrime & Cyber security trends and jurisprudence impacting cyberspace in today’s scenario.

4. To enable the participants appreciate, evaluate and interpret the case laws with reference to the IT Act and other Laws associated with the cyberspace.

5. To provide vivid knowledge about different types of Digital Forensics such as Mobile Device Forensics, Network Forensics, Cloud based Forensics etc., including the Standard Operating Procedures for IO’s which will be useful in investigating real-time cases pertaining to cybercrime.

6. To provide knowledge related to auditing of computer systems, managing and mitigating risk situations in the organization and techniques for investigating financial frauds.
Overview of Course

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Course Duration</th>
<th>Eligibility of the Participants</th>
<th>Minimum Qualifications</th>
</tr>
</thead>
</table>
| P G Diploma in Cyber Crime and Law             | 1 Year          | 1. **For In-Service Officers:** Forensic Scientists working in various CFSLs/FSLs in Cyber Forensic Division, SI and above working in Cyber Cells in Police Departments.  
2. **For Other Students:** Bridging Course of One Week | Graduate in any relevant discipline of Science                                                |

1. Academic session starts in August.
2. There are 2 semesters in each Academic Session. Semester 1 (August to November) and Semester 2 (January to April).
3. Examinations are held in the month of May and December.
4. Each semester consists of 17 weeks of teaching.
5. No. of teaching hours per week = 6 hours/day x 5 days/week = 30 hours
6. Semester 1 consists of 5 theory papers (practical work included) and Semester 2 consists of 4 theory papers (practical work included) along with a dissertation project.
7. Total number of papers in PG Diploma Course = 10 papers (1 year duration)
8. The total credit points of 1 year (2 semesters) are 56 credit points.
SYLLABUS OF P.G. DIPLOMA COURSE IN CYBER CRIME & LAW

Credit Distribution Matrix

Semester I

<table>
<thead>
<tr>
<th>Paper Code</th>
<th>Paper Name</th>
<th>L*</th>
<th>T*</th>
<th>P**</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGDCCL 101</td>
<td>Fundamentals of Computers &amp; Networking</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 102</td>
<td>Introduction to Cyber-crime</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 103</td>
<td>Fundamentals of Computer &amp; Network Security</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 104</td>
<td>IT Act and other Laws for cyber-crime</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 105</td>
<td>Auditing, Risk Management and Financial Fraud Investigation</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total (credits)</strong></td>
<td></td>
<td>12</td>
<td>5</td>
<td>3</td>
<td>20</td>
</tr>
</tbody>
</table>

Semester II

<table>
<thead>
<tr>
<th>Paper Code</th>
<th>Paper Name</th>
<th>L*</th>
<th>T*</th>
<th>P**</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGDCCL 201</td>
<td>Digital Forensics</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 202</td>
<td>Mobile and Network Forensics</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 203</td>
<td>Cloud and Virtual Technology Security</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 204</td>
<td>Intellectual Property Rights and Privacy Laws</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>PGDCCL 205</td>
<td>Dissertation (Mini Project)</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td><strong>Total (credits)</strong></td>
<td></td>
<td>9</td>
<td>4</td>
<td>23</td>
<td>36</td>
</tr>
</tbody>
</table>

* Each theory class of 1 hour (1 hour of lecture and/or 1 hour of Tutorial respectively) hold 1 credit point.

** Each practical class of 2 hours holds 1 credit point.
FIRST SEMESTER
Unit I – Basics of Computers

Overview and working of computers, Generation and Classification of computers, Basics of computer hardware and software, Booting process in a computer, Computer memory and its classification, other peripherals devices and cards.

Unit II – Understanding computer Architecture


Unit III – Basics of Operating System


Unit IV – Basics of Networking

Reference Books

Semester-I, Paper II
PG Diploma Cyber Crime and Law
PGDCCL-102 Introduction to Cyber-crime
L=2, T=1, P=1 Credits = 4

Unit I

Unit II
Cybercrime against organization – Unauthorized access of computer, Password Sniffing, Denial-of-service (DOS) attack, Backdoors and Malwares and its types, E-mail Bombing, Salami Attack, Software Piracy, Industrial Espionage, Intruder attacks.


Unit III

Unit IV
**Reference Books**


Semester-I, Paper III
PG Diploma Cyber Crime and Law
PGDCCL-103 Fundamentals of Computer & Network Security
L=2, T=1, P=1 Credits = 4

Unit I – Introduction to Cyber Security

Unit II – Basics of Cryptography

Unit III – Network and Wireless Attacks
Unit IV – Network Security


Reference Books

Semester-I, Paper IV
PG Diploma Cyber Crime and Law
PGDCL-104 IT Act and other Laws for Cyber-crime
L=3, T=1, P=0 Credits = 4

Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law


Unit II: Regulatory Framework of Information and Technology Act 2000


Unit III: Offences and Penalties


Unit IV: Indian Evidence Act


Reference Books

2. Vikas Vashisht.; “Law and practice of intellectual property in India”
9. The Copyright Act, 1957
11. The Indian Evidence Act, 1872.
Semester-I, Paper V  
PG Diploma Cyber Crime and Law  
PGDCCL-105 Auditing, Risk Management and Financial Fraud Investigation  
L=3, T=1, P=0 Credits = 4

Unit I- Introduction to International Standards and Audit Methodology

Unit II - Risk Management

Unit III- Financial Fraud

Unit IV- Analysis, Evidence and Testimony
Review internal controls to safeguard assets, Conduct small business asset protection survey & make recommendations for preserving company assets. Fraud auditing services. Uncover financial statement fraud. Conduct white-collar crime investigations. Asset record reconstruction. Provide anti-money laundering and/or fraud training. Consult on civil and/or criminal litigation matters, including asset forfeiture issues. Assist legal counsel with plea negotiations involving drug trafficking, public corruption, money laundering, & currency structuring
Reference Books

SECOND SEMESTER
Unit I – Basics of Digital Forensics


Unit II – Cyber Crime Investigation


Unit III – Analysis of Digital Evidences

Basics of various email clients like Outlook, Lotus Notes, Thunderbird, and forensically relevant files for the same (in both Windows and MacBook OS).

**Unit IV – Windows and Linux Forensics**


Forensic Acquisition and analysis of Apple OS macbooks, and their various forensic artefacts (Plists), Function of File Vault, Keychain

**Reference Books**

Semester-II, Paper II
PG Diploma Cyber Crime and Law
PGDCCL-202 Mobile and Network Forensics
L=2, T=1, P=1 Credits = 4

Unit I – Introduction to Mobile Technologies

Asynchronous Transfer Mode (ATM), Wireless Application Protocol (WAP). Cellular technologies including Advanced Mobile Phone System (AMPS), Imode, Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) including features and relative strengths. Functions of Subscriber Identity Module (SIM), International Mobile Equipment Identity (IMEI), Bluetooth and Mobile Payment Gateways. Understanding of the mobile phone operating systems – Android, iOS, Windows. Basics of Rooting/Jailbreaking.

Unit II – Introduction to Mobile Eco-System Security


Unit III – Introduction to Mobile Forensics

Mobile Forensic, Types of Evidence present in mobile phones - Files present in SIM card, phone memory dump, and evidences in memory card. Seizure and Preservation of mobile phones and PDA. Mobile phone evidence extraction process, Data Acquisition Methods – Physical, Logical and File System Manual Acquisition. Good Forensic Practices, Mobile Forensic Investigation Toolkit. Tracking of mobile phone location. Analysis of mobile data like SMS, call logs,
contacts, media files, recordings and important mobile application data (IM Chats like whatsapp, telegram, iMessage, Email clients, Calendar, Reminder and Note apps). Challenges to Mobile forensics. CDR and IPDR analysis.

**Unit IV – Introduction to Network Forensics**


**Reference Books**

Semester-II, Paper III
PG Diploma Cyber Crime and Law
PGDCCL-203 Cloud and Virtual Technology Security
L=2, T=1, P=1 Credits = 4

Unit I: Introduction to Cloud Computing
Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs. private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

Unit II: Cloud Application Architecture
Technologies and the processes required when deploying web services; Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages.

Unit III: Cloud Services Management
Reliability, availability and security of services deployed from the cloud. Performance and scalability of services, tools and technologies used to manage cloud services deployment; Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

Unit IV: Cloud Security and Forensics
Analysis of Cases while deciding to adopt secure cloud computing architecture. Appropriate cloud requirements. Secure Cloud based service, Applications and development platform deployment so as to improve the total cost of ownership (TCO). Cloud Security Architecture, Identity and Access Management, Encryption and Key Management.

Data Collection, Live Forensics, Evidence Segregation, virtualized environments and proactive measures. Organizational Dimension- Internal staffing, External
Dependency Chains, Service Level Agreement, Multiple Jurisdictions and Tenancy. Investigative tools in the virtualized environment. Analysis- correlation, reconstruction, time synchronization, logs, metadata, timelines. Cloud Forensic Challenges.

**Reference Books**

Unit I

Unit II

Unit III
Introduction to Copyright- International Protection of Copyright and Related rights- An Overview (International Convention/Treaties on Copyright). Indian Copyright Law- The Copyright Act, 1957 with its amendments, Copyright works, Ownership, transfer and duration of Copyright, Renewal and Termination of Copyright, Infringement of copyrights and remedies.

Unit IV

Reference Books
1. Vikas Vashishth.; “Law and practice of intellectual property in India”
4. The Copyright Act, 1957
The students would develop their project individually and get the topic approved by the Director. For the purpose of approval, they have to submit their project titles and proposals with the name of internal or external guides within twenty one days of the commencement of the semester. 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.

The students have to report to the guide for at least five 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 Director shall award the marks out of 20 on the basis of the Presentation, Demonstration, Viva-Voce, and basis of Project Report. The internal guide shall award out of 40 Marks.
Syllabus

Of

Post-Graduate Diploma in Cyber Crime and Law

(2018)

LNJN National Institute of Criminology & Forensic Science

Ministry of Home Affairs, Govt. of India

Delhi