

**M. Com. Part I (Semester II)**

**Group B (Commercial Laws & Practices) - Special Paper III**

**Subject Name: - E-Security and Cyber Laws**

**Course Code: - 105-II**

**Objectives of the course**

1. To make the students aware of the cyber wrongs/crimes;
2. To impart knowledge of e-security and Internet Security amongst students
3. To make student familiar with various provisions of cyber Laws and Information Technology Act
4. To make the students acquainted with the regulatory regime in computer field/e-business.

**Depth of the Programme:** – Fundamental Knowledge with insight to solve practical problems in Cyber laws and related issues

**Objective of the Programme:**

1. To equip and train Post Graduate students to accept the challenges of Business World by providing opportunities for study and analysis of advanced Commercial and business methods and processes.
2. To develop independent logical thinking and facilitate personality development.
3. To equip the students to opt for suitable careers in management and entrepreneurship.
4. To acquaint the students with methods of Data collection and their interpretations.
5. To develop among students Communication, Study and Analytical skills.

| <b>Unit No</b> | <b>Unit Title</b>                      | <b>Contents</b>   | <b>Purpose Skills to be developed</b>   |
|----------------|--|---|---|
| 1              | <b>Introduction to Computer crimes</b> | Computer Crimes. Types of Computer crimes, Specific Threats, Attacks on Computer Systems, Major types of Security Problems / Common threats, Computer Frauds and abuse techniques. Characteristics and types of computer frauds.<br><br>Preventing Computer Frauds and Ethical Considerations. System Vulnerability and abuse – Internet Vulnerability. Protecting Information systems from potential threats. E- Commerce security issues. Risk Involved in E- Commerce. Protecting E-Commerce System. | To understand the nature of different Computer Crimes and ways to protect systems from them and become aware of E-Commerce systems and Issues |

|   |   |  |  |
|---|---|--|--|
| 2 | <b>E-Security</b>   | <p>Introduction to E-Security and Security Requirements. Types of Intruders, attacking methods, Hackers and Crackers. Computer Viruses, Spam, Denial of services. Security Policy, Secure E-Transactions. Types of Information Systems Controls- General Controls – Physical Controls, Access Controls, Biometric Controls, data Security Controls and Application Controls. Security Tools and Methods- Password, Authentication, Access Control, Encryption,</p> <p>Firewall, Antivirus Software, Digital Identity and digital Signature, Digital Signature Certificate. Secure Socket Layer and Secure Electronic Transaction Protocols.</p>  | <p>To get acquainted with various concepts relating to E-Security and to understand different threats to E-Transactions, security measures, Information System Controls and Secure Electronic Transaction Protocol</p>                                   |
| 3 | <b>Cyber Laws (Information Technology Act, 2000) Part-I</b> | <p>Introduction to Cyber Laws—Meaning &amp; scope of Cyber Laws, online contracts, Requirements &amp; legal aspects of e-contracts ( offer and acceptance in e-form), Cyber Laws &amp; legal issues ( cyber jurisprudence, &amp; sovereignty, net neutrality, freedom of speech in cyber space, governance) Information Technology Act – 2000 Part-I Digital Signature-definition ,meaning, functions, procedure, E- Governance ( Ss. 4 to 9 ), E- Records ( Ss 11 to 16 ), Controller of Certifying Authority (powers, functions u/s 17 to 20), Digital Signature Certificates, License to issue Digital Signature Certificates, (suspension, revocation etc.-- Ss.21 to 26), Duties of Certifying Authority (Ss.30 to 34), Provisions relating to Digital Signature Certificates (Ss. 35 to 39), Duties of subscriber.</p> | <ul style="list-style-type: none"> <li>• To introduce Students about Cyber Laws legality of E- Transactions.</li> <li>• To study various legal provisions of the Information Technology Act relating to E-Governance, Digital signatures etc.</li> </ul> |

|   |  |  |   |
|---|--|--|---|
| 4 | <b>Cyber Laws (Information Technology Act, 2000) Part-II</b> | Penalties for Cyber wrongs and Adjudication (Ss. 43 to 47), Cyber Regulation Appellate Tribunal (Procedure and Powers (Ss.48 to 51, 57 to 64) Cyber Crimes/Offences & punishment (u/s 65 to 79), Offences by Companies (S.85) Amendments effected in IPC 1860, Indian Evidence Act, 1872, Bankers Books Evidence Act, 1891, Reserve Bank of India Act, 1934 pursuant to Ss. 91 to 94 of ITA, 2000. | To get sensitized on various penalties for the cyber wrongs provided in the Information Technology Act, 2000 and relevant amendments in certain other Laws. |
|---|--|--|---|

**\*All Acts are to be studied with recent amendments**

\*\*\*\*\*