**Program Elective – 1**

**Subject Code: 01CY0108**

**Subject Name:** Cyber Laws and Security Policies

 **MTech. Year – 1 (Semester – 1)**

**Objective:** After learning the course the students should be able to understand types of cyber law, IT Act, Security Policies and also how to protect them self and ultimately society from cyber threats

**Credits Earned:** 4 Credits

**Course Outcomes:** After completion of this course, student will be able to

* Explore the Legal and Policy Developments in Various Countries to Regulate Cyberspace.
* Develop and understanding of Relationship Between Commerce Learners in Depth Knowledge of Information Technology Act and Legal Frame Work of Right to Privacy, Data Security and Data Protection.
* Make Study on Various Case Studies on Real Time Crimes.

**Pre-requisite of course:** NA.

**Teaching and Examination Scheme**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Teaching Scheme (Hours) | Credits | Theory Marks | Tutorial/ Practical Marks | Total Marks |
| Theory | Tutorial  | Practical | ESE (E) | Mid Sem (M) | Internal (I) | Viva (V) | Term work (TW) |
| 3 | 0 | 2 | 4 | 50 | 30 | 20 | 25 | 25 | 150 |

**Contents**

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Contact Hours** |
| 1 | Introduction to cybercrime and cyber law, cyber space and information technology, Nature and scope of cybercrime, Jurisdiction of cybercrime. Important definitions under IT Act 2000, Cybercrime issues: unauthorized access, White collar crimes, viruses, malwares, worms, Trojans, logic bomb, cyber stalking, voyeurism, obscenity in internet, Software piracy.IT Act 2000, offences under IT Act and IT (amendment) Act, 2008. CRPC overview, Case studies, Role of intermediaries, Electronic evidence, Cyber terrorism, espionage, warfare and protected system | 12 |
| 2 | Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations | 10 |
| 3 | Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.  | 10 |
| 4 | Information security: fundamentals-Employee responsibilities information classification Information handling- Tools of information security- Information processing-secure program administration. Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals. | 10 |
|  | **Total Hours** | **45** |

TEXT BOOKS

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)”, 2nd Edition, O’ Reilly Media, 2006.

 2. Thomas R. Peltier, “Information Security policies and procedures: A Practitioner’s Reference”, 2nd Edition Prentice Hall, 2004.

REFERENCES:

1. Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global, 2009.

 2. Jonathan Rosenoer, “Cyber law: the Law of the Internet”, Springerverlag, 1997.