Information Technology Syllabus
Semester II

Course prerequisites: Working knowledge of Computer and Internet

Course objectives: Develop an awareness and understanding of Cyber Security and its related aspects and how to take measures to protect individual privacy and prevent loss/theft of data.

Course contents: Total: 60 Hours

I Basics of Computer Networking (10%): Marks: 10 & Lectures 08
Networking basics, why networking of computer is needed, Internet – role and importance, IP Addressing – public Vs Private, Static Vs Dynamic; WWW & related protocols;

II Emerging threats in Cyber Space (20%): Marks: 20 & Lectures 15
Threats in Cyber Space, Classification of threats, BYOD and portable devices threats, 0-day attacks, insider threats, Cyber Warfare, Malware threats, mobile apps threats;

Social media and its safe usages: Social media- its usages, Social networking- types, usages, importance, social networking safety;

III Online Privacy: (10%) Marks: 10 & Lectures 07
Privacy – basic concepts, Sensitive personal information, Privacy policies, Google/Facebook privacy policies, Privacy laws, IPR, Ethics & safe practices

IV Cyber Crimes – an introduction: (20%) Marks: 20 & Lectures 15
Introduction – types of cyber crimes, its impact – social, personal, financial; Types of Cyber Crimes (Phishing, social engineering, Denial of Service, Cyber stalking, ID-theft, etc), Cyber Terrorism, How to report cyber crimes

V Cyber Laws: (20%) Marks: 20 & Lectures 15
Evolution and purpose, offence & defence, bailable and non-bailable offences, provisions related to e-commerce, provisions for cyber crimes, adjudicating officers, CERT-IN- its role and powers

VI Cyber Forensic: (20%) Marks: 20 & Lectures 15
Data recovery, evidence collection, cloning of devices, media sanitization

Reference Books

**Web Resources:**
1. www.cert.org
2. www.microsoft.com/security/
3. www.nist.gov
4. www.sans.org
5. www.us.cert.gov