| Module Name (Computer Engineering/IT) | Total Hours |
|---|---|
| **Information & Cyber Security Assurance** | **30** |

| Topic | Sub Topic | Hours |
|---|---|---|
| 1. Introduction to Information and Cyber Security | 1.1 Basic of Internet<br>1.2 Information security: Need & Principals<br>1.3 OSI Model of Information Security<br>1.4 Security mechanisms and cryptography<br>1.5 Goals of Information security<br>1.6 Hands-on exercise of various networking commands<br>1.7 Demonstration of cryptography algorithms | 3 |
| 2. Desktop and Wireless Security | 2.1 Introduction to desktop security<br>2.2 Operating system Hardening - strong passwords, OS updates, software patches, system back-ups<br>2.3 Using anti virus, anti malware, firewall programs<br>2.4 Introduction to WLAN and WI-FI security<br>2.5 Types of attacks on wireless environment - DOS attack, man in middle attack, War driving<br>2.6 Guidelines for wireless communications<br>2.7 Hands on Exercises:<br>(1)Update your windows OS version by using patch/crack.<br>(2) Apply Some Inbound/Outbound Rules to your Desktop Firewall.<br>(3) Setup your Wireless Router at your home or institute.<br>(4) Monitor your wireless traffic using wireshark tool. | 6 |
| 3. Malicious Applications | 3.1 Malware, Types of Malware<br>3.2 Guidelines for preventing from Malware<br>3.3 Computer Viruses: Concepts, Life Cycles, Types<br>3.4 Possible ways to get virus in computer<br>3.5 Key loggers (Hands on exercise by using Actual Key Logger)<br>3.6 Trojans, Worms, Spyware, Adware<br>3.7 Hands on Exercise :Virus Analysis using Virus Total | 4 |
| 4. E-Mail and Browser Security: Threats and Countermeasures | 4.1 Web Browser risks - Active X, java, plugins, Javascript, Clickjacking, Cookie<br>4.2 Methods for securing web browsers<br>4.3 Proxy Browsers (Case Study:Tor/Onion Browser)<br>4.4 Cross Site Scripting (XSS) Attack<br>4.5 Introduction to E-mail and E-mail protocols- SMTP , POP/IMAP,PGP,S/MIME<br>4.6 Threats through E-mail<br>4.7 E-mail Phising<br>4.8 E-mail Tracer<br>4.9 Risks involved in E-mail security and guidelines | 4 |
| 5. Social Engineering and Social Networking Security | 5.1 Introduction to Social Engineering<br>5.2 Case studies and ways to countermeasure Social Engineering<br>5.3 Introduction to Social Networking<br>5.4 Risks in Social Networking<br>5.5 Guidelines to avoid risks in Social Networking<br>5.6 Detecting Phishing using Netcraft/PhishTank | 4 |
| 6. Mobile Security | 6.1 Introduction to Mobile Security<br>6.2 Types of Threats<br>6.3 Mitigation against Mobile device and data security attacks<br>6.4 Mitigation against Mobile connectivity security attacks<br>6.5 Android OS security guidelines - Introduction to Android OS, Risks | 4 |

| Topic | Sub Topic | Hours |
|---|---|---|
| | involved in android OS,<br>6.6 Protecting Android devices - device hardening, Managing app permissions, secure WI-FI, screen locks, downloading and updating Apps, backup | |
| 7. Cyber Ethics | 7.1 Computer Ethics<br>7.2 Internet Ethics<br>7.3 Unethical behaviour in Internet and examples: Digital Plagarism, Piracy, Copyrights<br>7.4 Cyber Bullying<br>7.5 Cyber Crime<br>7.6 Cyber Safety<br>7.7 Safety measures for Ethics | 3 |
| 8 Cyber Crime and Laws | 8.1 Introduction to Cyber laws and Cyber Crimes<br>8.2 IT Act 2000/ Amendment act 2008<br>8.3 Cyber Crime sections and descriptions<br>8.4 Various case studies of Cybercrimes, Card Frauds, Data Frauds, Consumer Complaints, Consequences and Courts Verdict. | 2 |
| | **Total hours** | **30** |