Certificate Course in Information Security & Cyber Law

Group Code	**:** ISCF	**Group Name**	**:** Information Security & Cyber Forensic
Course Code	**:** CT01	**Course Name**	**:** Information Security & Cyber Law

Objective of the Course

The course will cover the basics of information security & spread awareness of this field to help the participants understand the importance of security in their daily lives in the IT field.

Duration of the Course (in weeks)	**:**	80 Hours
Minimum Eligibility Criteria and pre-requisites, if any	**:**	10+2 pass with knowledge of basics of Computers

Outline of Course

Sl. No.	**Topic**	**Minimum No. of Hours**
1.	Information Security	04
2.	Security Services, mechanism and attacks	10
3.	Physical and System Security	10
4.	Internet and Web Security Fundamental	20
5.	Network Security Fundamentals	20
6.	IT acts & Cyber laws	06

Theory/Lecture Hours	=	**60 Hrs.**
Practical/Tutorial/Lecture Hours	=	**20 Hrs.**
Total Hours	=	**80 Hrs.**

Detailed Syllabus

1. Information Security **04 Hrs**

Need of Information Security, Attributes of Information Security, Authentication, Confidentiality, Integrity, Availability, Non Repudiation.

Hands on Practical:
Data Encryption techniques and Hashing.

2. Security Services, mechanism and attacks **10Hrs**

Access Control, Threats and Vulnerabilities, Security Attacks, Unauthorized Access, Impersonation, Denial of Service, Malicious Software, Viruses, Worms, Trojan Horses.
Definitions, Types of authentication, Password Authentication, Password Vulnerabilities &Attacks: Brute Force & Dictionary Attacks. Password Policy & Discipline, Single Sign-on – Kerberos, Alternate Approaches, Biometrics: Types of Biometric Techniques: False Rejection, False Acceptance, Cross over Error Rates.

Hands on Practical:
Antivirus installation, Password management, User Account Control (Windows), Biometric techniques.

3. Physical and System Security **10Hrs**

Function of Operating system , Types of OS (Real time OS, Single User Single task OS, Single User-Multi tasking System, Multiuser System), Task of OS , Process, Memory Management, Device Management, Storage Management, Application Interface, User Interface, Security Weakness, Operating System, Windows Weakness, Hardening OS during Installation, Secure User Account Policy, Strong User Password Policy, Creating list of Services and Programs running on Server, Patching Software, Hardening Windows, Selecting File System, Active Directory / Kerberos, General Installation Rules.

Hands on Practical:
Vulnerability Scanning using Security Analyzer tools (Nessus & MBSA), Manual and Automatic Hardening.

4. Internet and Web security **20Hrs**

Web Servers and Browsers, HTTP, Cookies, Caching, Plug-in, ActiveX, Java, JavaScript, Secure Socket Layer (SSL), Secure Electronic Transaction (SET).

E-mail Risks, Spam, E-mail Protocols, Simple Mail Transfer Protocol (SMTP), Post office Protocol (POP), Internet Access Message protocol (ICMP).
Secured Mail: Pretty Good Privacy (PGP), S⁄MIME(Secure/Multipurpose Internet Mail Extensions)

Hands on Practical:
Setting up browser security, Email Encryption and Digital signature.

5. Network security Fundamentals 20Hrs

Network Devices: Switches, Routers, Firewalls, VPN Concentrators, Load Balancers, Proxies.
Network Protocol: Overview of IPV4 and IPV6, OSI Model, Maximum Transfer Unit, Internet Protocol (IP), Transport Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Domain Name System (DNS).
Network Design: Network Address Translation (NAT), Demilitarized Zone (DMZ), Subnetting, Switching, Virtual Local Area Network (VLAN).
Network Attack: Buffer Overflow, TCP Session, Hijacking, Sequence Guessing, Network Scanning.
IP Security overview and architecture.

Hands on Practical:
Using Networking tools, Firewall and Router setting.

6. IT acts and Cyber Laws 06 Hrs

IT Act: Salient Feature of IT Act 2000, Legal Provisions under the Information Technology Act,Recent amendments by the IT (Amendment Act) 2008, ActSection66(A, B, C, D, E, F), ITActSection67(A,B,C)

Books recommended for reference and reading:
Cryptography & N/W Security by William Stallings

Recommended Hardware:
Wireless Router, Unmanaged Switch, Finger Print Scanner

Recommended Software:
Window 2008 and later, Open Source Security Software