CHM-A level

A7. 1: I. T. Security (Duration 70 Hours)

Subject Prerequisites:
Basic understanding of computers and internet

Subject Outcome:
Subject contents are designed with an intention to provide knowledge about Information security, access controls, security policies and risk management with introduction to biometrics and digital signatures, with a overview of IT act 2000 and Cyber forensic

Section	Brief Contents	Duration (Hrs)
1. Introduction to Information security	Attributes of information security(confidentiality, integrity, Availability) Threats and vulnerabilities (unauthorized access, Denial of Service, Viruses, Trojans, etc.)	3
2. Authentication and access control	types of authentication (password, one time password, token based authentication, vulnerabilities and attacks, password policies,	5
3. Security policies and risk management	Access control techniques, mandatory access, discretionary access, access control list, role based access, access control structure, windows and Linux access controls	6
4. Digital signatures and biometrics	Digital signatures, certifying authorities, PKI, certificate installation, types of digital signature algorithm, introduction to biometrics, types of biometrics, why biometrics, biometric model, FAR, FRR, FTE, etc	7
5. Web security and application security	web server security, browser security, security in active content, SSL, secured mail, introduction to program security, operating system security, database security etc	5
6. Security policies, IT Act 2000 and Cyber forensic	Need of security policy, assets identification, risk management, security architecture, secure audits, secure backups, security awareness, training, Incident response, incident handling. IT act 2000 objectives, provisions, offences, cyber crimes, and introduction to cyber forensic	14

List of Experiments	1. Demonstrate strong password techniques 2. Demonstrate various information security threats 3. Demonstrate various kinds of authentication techniques 4. Demonstrate various types of access controls 5. Demonstrate access control in windows 6. Demonstrate access controls in Linux 7. Demonstrate working of digital signatures 8. Case study on biometric techniques 9. Demonstrate secured email 10. Case study on assets identification and risk assessment 11. Prepare a Incidence response report 12. Case study on Acts in IT act 2000 13. Case study on Cyber crimes discussed in IT act 2000 14. Case study on modus operandi of Cyber crimes 15. Demonstrate preventive and precautionary measures for one of cyber-crimes	30