GOVERNMENT OF TAMILNADU
DIRECTORATE OF TECHNICAL EDUCATION,CHENNAI
STATE PROJECT COORDINATION UNIT
(Established under Canada India Institutional Cooperation Project)

CURRICULUM

Course Name	**Information Security & Cyber Law**
Course Code	**CSE/2020/007**
Course Duration	60 Hours
Minimum Eligibility Criteria and Pre-requisites(if any)	ITI/10th/+2/Diploma/Graduates
Course Objectives	Training module has been designed to ➢ Understand the basics of information security ➢ Understand the basics of Cyber Law. ➢ Understand the importance of security in their daily lives in the IT field.
Course Outcomes	The outcomes of the course are as follows : • Apply fundamental concepts of Information Security threats and vulnerabilities to adopt right security measures • Implement, monitor and maintain a secure network consisting of enterprise level routers and switches.
Expected Job Roles	Network Admin

TEACHING AND SCHEME OF EXAMINATION

Course Code	Course Name	Hours		Assessment Marks		Duration of Examination
				Min	Max	
CSE/2020/007	**Information Security & Cyber Law**	Theory	20	10	20	3 Hours
		Practical	40	40	80	
		Total	60	50	100	

CSE/2020/007 - INFORMATION SECURITY & CYBER LAW

DETAILED SYLLABUS

UNIT NO	MODULES	NO.OF.HOURS THEORY
I	INTRODUCTION TO INFORMATION SECURITY	
1.1	Need for Information Security-Attacks, Threats	3
1.2	Attributes of Information Security, Authentication, Confidentiality, Integrity, Availability, Non Repudiation.	
1.3	Access Control, Threats and Vulnerabilities,	
1.4	Security Attacks, Unauthorized Access, Impersonation, Denial of Service, Malicious Software, Viruses, Worms, Trojan Horses.	
II	AUTHENTICATION	
2.1	Definitions, Types of authentication, Password Authentication, Password Vulnerabilities &Attacks: Brute Force & Dictionary Attacks.	4
2.2	Password Policy & Discipline, Single Sign-on – Kerberos	
2.3	Biometrics: Types of Biometric Techniques: False Rejection, False Acceptance, Cross over Error Rates.	
III	PHYSICAL AND SYSTEM SECURITY	
3.1	Function of Operating system, Types of OS, Task of OS , Process, Memory Management, Device Management, Storage Management, Application Interface, User Interface	5
3.2	Security Weakness, Operating System, Windows Weakness, Hardening OS during Installation, Secure User Account Policy, Strong User Password Policy	
3.3	Creating list of Services and Programs running on Server, Patching Software, Hardening Windows, Selecting File System, Active Directory / Kerberos, General Installation Rules.	
IV	INTERNET AND WEB SECURITY	
4.1	Web Servers and Browsers, HTTP, Cookies, Caching, Plug-in, ActiveX, Java, JavaScript,	5
4.2	E-mail Risks, Spam, E-mail Protocols, Simple Mail Transfer Protocol (SMTP), Post office Protocol (POP), Internet Access Message protocol (ICMP).	
4.3	Secured Mail: Pretty Good Privacy (PGP), S/MIME(Secure/Multipurpose Internet Mail Extensions)	
4.4	Secure Socket Layer (SSL), Secure Electronic Transaction (SET).	
V	IT ACTS AND CYBER LAWS	
5.1	Salient Feature of IT Act 2000, Legal Provisions under the Information Technology Act.	3
5.2	Recent amendments by the IT (Amendment Act) 2008, ActSection66(A, B, C, D, E, F), ITActSection67(A,B,C)	
	Total Theory Hours	**20**
	Total Practical Hours	**40**
	Total Hours	**60**

PRACTICAL (40 HOURS)

1. Implementing access rights for files and folders.
2. Implementing encryption for a file.
3. Installing different authentication devices fingerprint scanner, face detection
4. Familiarizing with biometric database, templates and analyzing data.
5. Implement Data Encryption techniques like Substitution cipher and Caesar cipher.
6. Implement Data Encryption techniques like Transposition cipher and Play fair cipher.
7. Implement Digital Signature.
8. Antivirus installation in an O S.
9. Password management and User Account Control (Windows)
10. Vulnerability Scanning using Security Analyzer tools.
11. Manual and Automatic Hardening.
12. Setting up browser security.
13. Email Encryption
14. Using Networking tools, Firewall and Router setting.
15. Practical Use of Network Security Tools, Email Header Analysis, configuration of network security equipment such as firewall, routers, IDS, Wireless Access Points

HARDWARE REQUIREMENT

S.NO	LIST OF TOOLS /EQUIPMENTS
1	COMPUTER WITH ANY OPERATING SYSTEM
2	PRINTER
3	SCANNER
4	PHOTO TYPE SETTING
5	LAN CONNECTION WITH INTERNET
5	ROUTER

SOFTWARE REQUIREMENT

S.NO	LIST OF SOFTWARE
1	OPERATING SYSTEM (WINDOWS)
2	ANTIVIRUS
3	DIGITAL SIGNATURE SOFTWARE

REFERENCE BOOKS

S.NO	NAME OF THE BOOK	AUTHOR	PUBLISHER
1.	Network Security Essentials (3rd Edition)	Stallings	Prentice Hall, 2007
2.	Firewalls and Internet security (2nd edition)	W.R.Cheswick and S.M.Bellovin	Addison-Wesley, 2003

ASSESSMENT AND CERTIFICATION

S.No	Criteria for assessment
1.	A trainee will be assessed based on the performance in End Examination for Theory and Practical conducted internally in the Project Polytechnic College for a duration of 3 hours
2.	A trainee must have 75% of attendance to appear for End examination in Theory and Practical.
3.	The assessment for theory part will be based on the marks scored in the end examination on the knowledge bank of questions (1 word/objective type questions)
4.	The assessment for practical part will be based on the marks scored in the end examination conducted by the Project Polytechnic and assessed by the Examiners approved by Strategic Plan Implementation Committee (SPIC) of the project polytechnic.
5.	The criteria for successful completion of training is every trainee should score 50% of marks in theory and practical examination.
6.	On successful completion of training , Certificate will be issued to the participants by the Directorate of Technical Education through the Project Polytechnic.

END EXAMINATION

ALLOCATION OF MARKS

S.No	Description	Max.Marks
1.	Theory Examination	20
2.	Practical Examination	
	a)Procedure	10
	b)Execution	30
	c)Output	20
	d)Record	20
	Total Marks	**100**

THEORY MODEL QUESTION PAPER

CSE/2020/007 - INFORMATION SECURITY & CYBER LAW

(Maximum Marks : 20)

(N.B: Answer any **twenty** questions) **20 x 1 = 20 Marks**

1. Write any two attributes of Information Security.
2. What is Authentication?
3. What is Confidentiality?
4. What is Non Repudiation?
5. Write any two attack types.
6. What is DoS attack?
7. What is the purpose of Brute force attack?
8. What is Dictionary attack used for?
9. Write any two Biometric traits
10. What is False acceptance?
11. What is False rejection?
12. What is Cross over error rate?
13. Write any two functions of OS?
14. Name any two OS types.
15. What are Cookies in Web?
16. Write any two advantages of Caching.
17. Write any two E-mail protocols.
18. What is the use of PGP?
19. What is the use of SSL?
20. Where is SET used?
21. Which section of IT Act 2000 deals with Computer Hacking?
22. Which section deals with Digital signature?
23. What is punishment for hacking of computers?
24. Which section deals with Credit card Fraud?
25. When did IT act come into effect?