DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
(AUTONOMOUS)
(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
Re-Accredited with 'A' Grade By NAAC, Accredited by TCS.
Accredited by NBA (AERO, CSE, IT & MECH)
Re-Accredited by NBA (BME, ECE, EEE)
PERAMBALUR - 621212.

COURSE PLAN (2025-2026)

Name of the Faculty Members				
Designation/Department	ASSISTANT PROFESSOR /IT			
Course Code/Name	U23CST64/INFORMATION SECURITY			
Year/Section/Department	III / IT / A & C			
Credits Details	L:3	T:0	P:0	C:3
Total Contact Hours Required	45			

Syllabus:

UNIT-I INTRODUCTION	**9**
History, What is Information Security? Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC	
UNIT-II SECURITY INVESTIGATION	**9**
Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues- An Overview of Computer Security - Access Control Matrix, Policy-Security policies, Confidentiality policies, Integrity policies and Hybrid policies	
UNIT–III SECURITY ANALYSIS	**9**
Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk -Systems: Access Control Mechanisms, Information Flow and Confinement Problem.	
UNIT-IV LOGICAL DESIGN	**9**
Blueprint for Security, Information Security Policy, Standards and Practices, ISO 17799/BS7799 NIST Models, VISA International Security Model, Design of Security Architecture, Planning for Continuity.	
UNIT-V PHYSICAL DESIGN	**9**
Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices, Physical Security, Security and Personnel	

TOTAL: 45 PERIODS

Objectives:

The main learning objective of this course is to prepare the students:

- To introduce information security concepts, models, and the security SDLC.
- To explore security investigation, business needs, and legal/ethical issues in security.
- To study risk management, access control mechanisms, and the confinement problem.
- To understand security policy, standards, and design for continuity.
- To explore physical security technologies, cryptography, and access control devices.

Text Book(s):

1. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, 2021.
2. Evan Wheeler, "Security Risk Management: Building an Information Security Risk Management Program from the Ground Up", First edition, Syngress Publishing, 2011

Reference Books:

1. Micki Krause, Harold F. Tipton, " Hand book of Information Security Management", Vol 1-3 CRC Press LLC, 2004
2. Stuart McClure, Joel Scrambray, George Kurtz, "Hacking Exposed", Tata Mc GrawHill,2003
3. Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002.

NPTEL LINK:

https://onlinecourses.swayam2.ac.in/cec22_cs15/preview

WEB SOURCES:

W1:https://www.slideshare.net/slideshow/it8073-information-security-unit-i-full-notes/266535484
W2:https://www.studocu.com/in/document/ramco-institute-of-technology/data-and-information-security
W3:https://www.scribd.com/presentation/948606806/UNIT-1
W4:https://www.brainkart.com/article/NSTISSC-Security-Model_7917

Course Plan:

Topic No	Topic Name	Reference Detail	Page No	Teaching Methodology	No of periods required	Cumulative periods
UNIT I	**INTRODUCTION**					**(9)**
1.	History	R1	3-4	**BB** Black Board	1	1
2.	What is Information Security?	R1	10-12	**BB/ PPT**	1	2
3.	Critical Characteristics of Information	R1	14-17	**BB/ PPT**	2	4
4.	NSTISSC Security Model	W5	WEB	**BB/ PPT**	1	5
5.	Components of an Information System	R1	20-23	**BB/ PPT**	1	6
6.	Securing the Components	R1	38-40	**BB/ PPT**	1	7
7.	Balancing Security and Access	R1	40-42	**BB/ PPT**	1	8
8.	The SDLC	R1	25-29	**BB/ PPT**	1	9
9.	The Security SDLC	R1	31-38	**BB/ PPT**	1	10
Outcome of Unit-I	Discuss the basics of information security.					
UNIT II	**SECURITY INVESTIGATION**					**(9)**

10.	Need for Security, Business Needs	R3	9-10	**BB/ PPT**	1	11
11.	Threats, Attacks, Legal Issues	R3	6-20	**BB/ PPT**	1	12
12.	Ethical and Professional Issues	R3	16-21	**BB/ PPT**	1	13
13.	An Overview of Computer Security	R3	3-6	**BB/ PPT**	1	14
14.	Access Control Matrix	R3	31-36	**BB/ PPT**	1	15
15.	Policy-Security policies	R3	109-117	**BB/ PPT**	1	16
16.	Confidentiality policies	R3	141-158	**BB/ PPT**	1	17
17.	Integrity policies	R3	173-177	**BB/ PPT**	1	18
18.	Hybrid policies	R3	227-236	**BB/ PPT**	1	19

Outcome of Unit-II Illustrate the legal, ethical and professional issues in information security

UNIT III	**SECURITY ANALYSIS**					**(9)**
19.	Risk Management	R3	3-19	**BB/ PPT**	1	20
20.	Identifying Risk	R1	200	**BB/ PPT**	1	21
21.	Assessing Risk	R1	204	**BB/ PPT**	1	22
22.	Assessing and Controlling Risk	R1	208	**BB/ PPT**	1	23
23.	Systems Mechanisms	R1	209	**BB/ PPT**	1	24
24.	Access Control Mechanisms	R1	228	**BB/ PPT**	1	25
25.	Information Flow	R4	267	**BB/ PPT**	1	26
26.	Confinement Problem	R4	415	**BB/ PPT**	1	27

Outcome of Unit-III: Explain the basics of risk assessment and control**.**

UNIT –IV	**LOGICAL DESIGN**					**(9)**
27.	Blueprint for Security	T2	259-285	**BB**	1	28
28.	Information Security Policy	W2	-	**BB**	1	29
29.	Standards and Practices	W2	-	**BB/ PPT**	1	30
30.	ISO 17799/BS7799	W4	-	**BB/ PPT**	1	31
31.	NIST Models	W2	-	**BB/ PPT**	1	32
32.	VISA International Security Model	W2	-	**BB/ PPT**		33
33.	Design of Security Architecture	W2	-	**BB/ PPT**		34
34	Planning for Continuity	W2	-	**BB/ PPT**		35

Outcome of Unit-IV: Describe various security models, standards and frameworks

UNIT –V	**PHYSICAL DESIGN**	**(9)**				
37.	Security Technology	W2	-	**BB**	1	36
38.	IDS	W2	-	**BB/ PPT**	1	37
39.	Scanning Tools	W2	-	**BB/ PPT**	1	38
40.	Analysis Tools	W2	-	**BB/ PPT**	1	39

41.	Cryptography	W2	-	**BB/ PPT**	1	40
42.	Access Control Devices	W2	-	**BB/ PPT**	1	41
43.	Physical Security,	W2	-	**BB/ PPT**	1	42
44.	Security	W4	-	**BB/ PPT**	2	44
45.	Personnel.	W2	-	**BB/ PPT**	1	45
Outcome of Unit-V	Illustrate the tools that are used for security analysis.					

Course Outcomes - Program Outcome Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	-	-	-	-	-	-	1	-	2	2	1
CO2	2	3	1	2	-	3	-	3	-	1	-	2	1	1
CO3	2	3	2	3	2	-	-	-	-	1	-	2	2	2
CO4	2	2	3	2	2	1	-	-	1	2	2	2	2	3
CO5	2	2	3	2	3	1	-	-	-	1	1	2	3	3
CO6	1	1	-	-	-	3	2	3	2	2	1	3	1	1
Avg	2	2	2	2	2	2	2	3	2	1	1	2	2	2

[Levels of correlation: 3(High), 2(Medium), 1(Low)]

Assignment:

Register Number	Total Number	Mode of Assignment MCQ/Seminar/PPT	Topics
Assignment:1			
	64 +66	Written	• NSTISSC Security Model • The SDLC
Assignment:2			
	64+66	PPT	• An Overview of Computer Security • Access Control Matrix
Assignment:3			
	64+66	Seminar	• Assessing and Controlling Risk • Access Control Mechanisms
Assignment:4			
	64+66	Case study	• IDS • ISO 17799/BS7799 • Cryptography
Assignment:5			
	64+66	MCQ	• All five Units

Submission Details:

Phase 1(Before AT 1)		Phase 2 (Before AT 2)		Phase 3 (Model)
Assignment 1	Assignment 2	Assignment 3	Assignment 4	Assignment 5

PLAN OF ASSESSMENT TEST –DISTRIBUTION OF MARKS:

TEST	CO- MARK WISE DISTRIBUTION						BLOOM'S LEVEL MARK WISE DISTRIBUTION					
AT-1	CO1	CO2	CO3	CO4	CO5	CO6	BTL1	BTL2	BTL3	BTL4	BTL5	BTL6
	37	23	--	--	--	--	21	23	16	--	--	--
AT-2	CO1	CO2	CO3	CO4	CO5	CO6	BTL1	BTL2	BTL3	BTL4	BTL5	BTL6
	--	--	37	23	--	--	--	--	--	--	--	--
MODEL	CO1	CO2	CO3	CO4	CO5	CO6	BTL1	BTL2	BTL3	BTL4	BTL5	BTL6
	20	20	20	20	20	--	--	--	--	--	--	--

Google Class Code Details:

Class Name: U23CST64-INFORMATION SECURITY

Class Code: edzojwri

Prepared by
AP/IT

Verified By
HOD/IT

Approved By
Principal