MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

COURSE PLAN

Department	:	Information & Communication Technology
Course Name & code	:	Cyber Security & ICT 3156
Semester & branch	:	V & IT
Name of the faculty	:	Mrs. Manjula C Belavagi and Dr. Krishna Prakasha K
No of contact hours/week:	:	L: 3, T: 0, P: 0, C: 3

Course Outcomes (COs)

	At the end of this course, the student should be able to:	No. of Contact Hours	Marks
CO1:	Understand the basics of cyber security.	9	25
CO2:	Evaluate attacks on operating system, network, and web.	7	20
CO3:	Analyze the existing vulnerabilities and propose solutions.	12	34
CO4:	Examine real case studies of cyber security incidents and their mitigation.	8	21
CO5:			
	Total	36	100

Assessment Plan

Components	Assignments	Sessional Tests	End Semester/ Make-up Examination
Duration	20 to 30 minutes	60 minutes	180 minutes
Weightage	20 % (4 X 5 marks)	30 % (2 X 15 Marks)	50 % (1 X 50 Marks)
Typology of Questions	Understanding/ Comprehension; Application; Analysis; Synthesis; Evaluation	Knowledge/ Recall; Understanding/ Comprehension; Application	Understanding/ Comprehension; Application; Analysis; Synthesis; Evaluation
Pattern	Answer one randomly selected question from the problem sheet (Students can refer their class notes)	MCQ: 10 questions (0.5 marks) Short Answers: 5 questions (2 marks)	Answer all 5 full questions of 10 marks each. Each question may have 2 to 3 parts of 3/4/5/6/7 marks
Schedule	4, 7, 10, and 13th week of academic calendar	Calendared activity	Calendared activity
Topics Covered	Quiz 1 (L_{x1-x2} & T_{y1-y2}) **(CO x)** Quiz 2 (L_{x3-x4} & T_{y3-y4}) **(CO x)** Quiz 3 (L_{x5-x6} & T_{y5-y6}) **(CO x)** Quiz 4 (L_{x7-x8} & T_{y7-y8}) **(CO x)**	Test 1 (L_{a1-a2} & T_{b1-b2}) **(CO x)** Test 2 (L_{a3-a4} & T_{b3-b4}) **(CO x)**	Comprehensive examination covering full syllabus. Students are expected to answer all questions **(CO1-5)**

Lesson Plan

L. No./ T. No.	Topics	Course Outcome Addressed
L0	Introduction to the Course	
L1	Introduction: Basics of Computer security, Confidentiality, Integrity, Availability.	CO1
L2	Introduction: Threats, Harms, Vulnerabilities, Controls, Conclusion.	CO1
L3	Authentication- Identification Vs Authentication, Authentication Based on Phrases and Facts.	CO1, CO2
L4	Authentication Based on Biometrics, Authentication Based on Tokens, Federated Identity Management.	CO1, CO2
L5	Multifactor Authentication, Secure Authentication, Access Control- Access Policies.	CO1
L6	Implementing Access Control, Existing Access Control Models.	CO1
L7	Cryptography- Terminology, Symmetric and Asymmetric Encryption- AES, DES.	CO1
L8	RSA, Message Digests, Key Exchange, Certificates, Digital Signatures.	CO1
L9	Programming Insights: Non-malicious programs.	CO1, CO3
L10	Programming Insights: Viruses.	CO1, CO3
L11	Programming Insights: Worms.	CO1, CO3

L12	Programming Insights: Trojans, Countermeasures.	CO1, CO3
L13	Basics of hacking, Phishing, Brute Force Attack.	CO3
L14	Denial of Service, Distributed Denial of Service.	CO3
L15	Attacks, Penetration Testing.	CO3
L16	Bots and Botnets.	CO3
L17	Browser Attacks, Web Attacks targeting Users.	CO2
L18	Obtaining Users or Website Data, Email Attacks.	CO2
L19	Security in Operating System.	CO2
L20	Security in the Design of Operating Systems, Rootkit.	CO2
L21	Network Security Attacks.	CO2
L22	DoS, DDoS.	CO2
L23	Browser Encryption, Onion Routing.	CO3
L24	IP Security Protocol Suite (IPsec), Virtual Private Networks.	CO3
L25	Firewalls, Intrusion Detection and Prevention Systems.	CO3
L26	Network Management.	CO3
L27	Security Planning, A Measurement Primer for Cybersecurity, Handling Incidents.	CO3, CO4
L28	Risk Analysis, Risk Matrices, Lie Factors.	CO3, CO4
L29	Misconceptions, and Other Obstacles to Measuring Risk.	CO4
L30	Cyber Crime & Cyber Terrorism: Definitions, Emerging Threats.	CO3, CO4
L31	Ethical Issues in Computer Security.	CO4
L32	Incident Analysis with Ethics.	CO4
L33	Case Studies on Cyber Crime & Cyber Terrorism.	CO4
L34	Case Studies on Cyber Crime & Cyber Terrorism.	CO4
L35	Case Studies on Cyber Crime & Cyber Terrorism.	CO4
L36	Case Studies on Cyber Crime & Cyber Terrorism.	CO4

References:

1.	Pfleeger C. P., Pfleeger S. L. and Margulies J., Security in Computing (5e), Prentice Hall, 2015.
2.	Akhgar B., Staniforth A. and Bosco F., Cyber Crime and Cyber Terrorism Investigator's Handbook (1e), Syngress Publishing, 2014.
3.	Hubbard D. W. and Seiersen R., How to Measure Anything in Cybersecurity Risk, John Wiley & Sons, 2016.
4.	Mitnick K. D. and Simon W. L., Art of Intrusion, Wiley Publishing Inc. 2005.
5.	Singer P. W. and Friedman A., Cybersecurity and Cyber war- What Everyone Needs to Know, Oxford.
6.	
7.	

Submitted by: Mrs. Manjula C Belavagi and Dr. Krishna Prakasha K

(Signature of the faculty)

Date: 06-08-2021

Approved by: Dr. Smitha N Pai

(Signature of HOD)

Date: 06-08-2021

FACULTY MEMBERS TEACHING THE COURSE (IF MULTIPLE SECTIONS EXIST):

FACULTY	SECTION	FACULTY	SECTION
Mrs. Manjula C Belavagi	A		
Dr. Krishna Prakasha K	B		