

Programme : Diploma in Computer Engineering and Information Technology (Sandwich Pattern)												
Course Code: CO23114						Course Title: Computer Security						
Compulsory / Optional: Compulsory												
Teaching Scheme and Credits						Examination Scheme						
CL	TL	LL	SLH	NLH	Credits	FA-TH TH1 TH2	SA-TH (2Hrs.30 Min)	FA- PR	SA PR OR		SLA	Total
03	-	02	01	06	03	20 20	60	25	25#	-	25	175

Abbreviations: CL- Classroom Learning, TL- Tutorial Learning, LL- Laboratory Learning, SLH-Self Learning Hours, NLH-Notional Learning Hours, FA - Formative Assessment, SA -Summative assessment, SLA- Self Learning Assessment
 Legends: @ Internal Assessment, # External Assessment, *# Online Examination, @\\$ Internal Online Examination

Note:

1. FA-TH represents Total of two class tests of 20 marks each conducted during the term.
2. FA-PR represents Tutorial Term work of 25 Marks
3. SLA represents self-learning Assessment of 25 Marks
4. SA-TH represents the end term examination of 60 Marks

I. Rationale

The aim of the course is to familiarize students with the basic problems of computer security. They will include the risks of information systems in the context of confidentiality, integrity and availability of information security policy development issues system, elements of cryptography, issues of electronic signatures and public key infrastructure, basic models of authentication, access control policies, security, communication protocols and application services.

II. Industry / Employer Expected Outcome

Students will be able to

- a) Protect an organization's computer systems, networks, and data from cyber threats.
- b) Develop secure system by using security algorithms and tools.

III. Course Outcomes: Students will be able to

- CO1 Identify the potential threats to confidentiality, integrity and availability of Computer Systems
 CO2 Use cryptography algorithms and protocols to achieve Computer Security
 CO3 Build systems that are more secure against attacks.
 CO4 Apply security principles to secure Operating Systems and applications.

IV. Course Content Details:

Uni t No.	Theory Learning Outcomes (TLO's)aligned to CO's.	Topics / Sub-topics
1	TLO 1.1 Understand the concept of computer security. TLO 1.2 Understand the principles of security. TLO 1.3 Understand various types of security attacks	Introduction to computer security and security trends. 1.1 Definition of Computer Security, Need for security, Security basics: Confidentiality, Integrity, Availability, Accountability, Non-repetition. Example of Security, Challenges for security. 1.2 Risk and Threat Analysis: Assets, Vulnerability, Threats, Risks, Counter measures. 1.3 Threat to Security: Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare, Avenues of attack, steps in attack 1.4 Security attacks: Active and Passive attacks, Denial of service, backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, encryption attacks, Keyloggers 1.5 Malware : Viruses, Logic bombs.
2	Course Outcome: CO1 TLO 1.1 Understand and apply core concepts of identification, authentication TLO 1.2 Understand the importance of security awareness TLO 1.3 Identify advantages and limitations of biometric authentication.	Teaching Hours: 06 Marks: 04 Identification, Authentication and Operational Security 2.1 Username and password, Managing passwords, choosing password. 2.2 Role of people in Security: Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software/hardware, Access Nonemployees, Security awareness, Individual User responsibilities 2.3 Access controls: Definition, principle, policies: DAC, MAC, RBAC. 2.4 Biometrics: fingerprints, handprints, Retina
Computer Security (CO23) Course Outcome: CO1		Teaching Hours: 06 Marks: 04 Approved Copy, Retina Teaching Hours: 06 Marks: 04

patterns, voice patterns, signature and writing patterns.



	Course Outcome: CO2		
4	TLO 1.1 Understand the working of Firewall & Kerberos	Teaching Hours: 13	Marks: 14
	TLO 1.2 Understand an Intrusion detection systems with it's types.	Computer Security Technology and Intrusion Detection	
	TLO 1.3 Understand E-mail security.	4.1 Firewalls: Need for Firewall, limitations, characteristics. Types of Firewalls: Hardware, Software, Packet filter, Proxy Server, Hybrid, Application gateways, circuit level gateway, Implementing Firewall.	
		4.2 Kerberos: Working, AS, TGS, SS	
		4.3 Intrusion Detection: Intrusion detection systems (IDS), host-based IDS, network-based IDS, Honey pots.	
		4.4 Email security: Email security standards: Working principle of SMTP, PGP, S/MIME.	
	Course Outcome: CO3	Teaching Hours : 08	Marks: 08

5 TLO 1.1 Understand the concept of computer security

TLO 1.2 Understand cyber laws.

TLO 1.3 Understand procedure & techniques of Cyber forensics.

Cyber Security

5.1 Introduction to Cyber Crimes – Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Mail Bombs, Bug Exploits, Cyber Crime Investigation

5.2 Introduction Cyber Laws- Introduction to IT act 2000 and IT act 2008, Introduction to the cyber laws.

5.3 Cyber Forensics: Introduction to Cyber Forensic, Forensic Tools and Techniques, Investigating the Crime Scene, Rules of Evidence.

Course Outcome: CO3

Teaching Hours: 06

Marks: 06

6 TLO 1.1 Understand application security

Application, Web & Database Security

TLO 1.2 Understand web security

6.1 Application hardening, application patches, web servers, active directory.

TLO 1.3 Understand & apply database security

6.2 Web security threats, web traffic security approaches, Secure socket layer and transport layer security, secure electronic transaction

6.3 Database Security: SQL Injection, Web Application & SQL Injection, SQL Injection prevention

Course Outcome: CO4

Teaching Hours: 06

Marks: 08

V. Laboratory Learning Outcome and Aligned Practical / Tutorial Experiences.

Sr No	Practical/Tutorial/ Laboratory Learning Outcome (LLO)	Laboratory Experiment / Practical Titles / Tutorial	Number of hrs.	Rel eva nt CO s
1	LLO 1.1. Demonstrate the use of malware and virus detection tools	Identify malwares and viruses from your system by using any malware/virus detection tool.	02	CO1
2	Computer Security (CO23) Keylogger	Use keylogger to get confidential data. (Approved Copy)	P-23 04 Scheme	CO1

3	LLO 3.1 Demonstrate the use of Cryptool	Create Digital Signature document using Cryptool	04	C02
4	LLO 4.1 Implement substitution technique.	Implement Caesar cipher algorithm	02	C02
5	LLO 5.1. Implement transposition technique	Implement rail fence technique & Simple columnar techniques.	04	C02
6	LLO 6.1 Apply RSA algorithm	Encrypt & decrypt a plaintext using RSA algorithm..	02	C02
7	LLO 7.1 Apply DH-key algorithm	Perform key exchange using DH algorithm	02	C02
8	LLO 8.1 Use tool for packet filtering	Filter packets according to protocol using any packet filtering tool..	02	C03
9	LLO 9.1 Demonstrate the use of following tools for network security	Demonstrate the use of following tools: <ul style="list-style-type: none">● Samspade● Nslookup● Whois● Tracert	04	C03
10	LLO 10.1. Able to demonstrate buffer overflow attack	Demonstrate buffer overflow attack.	02	C03
11	LLO 11.1. Demonstrate SQLInjection	Perform SQLInjection on any website (HTMLget)	02	C04
12	LLO 12.1.0 Able to analyze a real-world cybercrime case.	Case study of cyber-crime, where the attacker has performed any kind of cyber-attack. Prepare a report and also list the laws that will be implemented on attacker.	02	ALL

VI. Suggested Micro Project / Assignment/ Activities for Specific Learning / Skills Development (Self Learning):

1. Create a tool to find bugs on website.
2. Create a script that can detect the presence of a keylogger on endpoint.
3. Create a Phishing Awareness Simulation Tool

VII. Specification Table:

Unit No	Topic Title	(Approved Copy)	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks Scheme
Computer Security (CO23)			P-23			

1	Introduction to computer security and security trends.	4	4	-	8
2	Identification, Authentication and Operational Security	4	4	2	10
3	Cryptography	4	4	12	20
4	Computer Security Technology and Intrusion Detection	2	4	2	8
5	Cyber Security	2	4	-	6
6	Application, Web & Database Security	2	4	2	8
Total		18	24	18	60

VII. Assessment Methodologies/Tools

Formative Assessment (Assessment for Learning)

- TH- Progressive /Periodic Test each of 20 Marks
- TL - Continuous Assessment of Tutorials for 25 Marks
- SL - Continuous Assessment of Self Learning for 25 Marks

Summative Assessment (Assessment of Learning)

- TH - Term End examination of 60 Marks

VIII. Suggested COs - POs Matrix Form

Programme Outcomes (POs)

Course Outco mes (COs)	PO-5 Engineering Practices for Society, Sustainabilit y and Environment						PO-7 Life Long Learnin g
	PO-1 Basic and Discipline Specific Knowledge	PO-2 Proble m Analys is	PO-3 Design/ Developme nt of Solutions	PO-4 Engineerin g Tools	PO-6 Project Manageme nt	PO-7 Life Long Learnin g	
CO1	1	2	2	--	--	--	3
CO2	1	3	3	--	2	1	3
CO3	1	2	3	--	2	--	3
CO4	1	2	3	--	2	--	3

IX. Suggested Learning Materials / Books

Sr. No.	Computer Security (CO26)	Author, Publisher, Edition and (Approved Copy) Year Of publication	ISBN Scheme

01	Cryptography and Network Security	Atul Kahate	Tata McGraw Hill
02	Computer Security Principles and Practices	William Stallings,	Pearson Education
03	Principles of Computer Security + and Beyond	Wm. Arthur Conkin	Mc Graw Hill

X. Learning Websites & Portals

1. <http://www.pgpintro.org/doc/pgpintro>
2. <http://www.emailtrackerpro.com>
3. <http://www.kmint21.com>
4. <http://www.jjtc.com/Steganography/tools.ht>

XI. Academic Consultation Committee/Industry Consultation Committee:

S r.	Name	Designation	Institute/Organization
1	Mr. Atul Jadhav	Director	Cybernist Pvt Ltd.
2	Mrs Madhuri Arde	Lecturer in Information Technology	Govt. Polytechnic Kolhapur
3	Mrs R. V. Molawade	Lecturer in Computer Engineering	Govt. Polytechnic Mumbai

Coordinator,
Curriculum Development,
Department of Computer Engineering

Head of Department
Department of Computer Engineering

I/C, Curriculum Development Cell
Government Polytechnic, Mumbai

Principal
Government Polytechnic, Mumbai