Lovely Professional University, Punjab

Course Code	Course Title	Course Planner	Lectures	Tutorials	Practicals	Credits
INT407	INFORMATION SECURITY AND PRIVACY	17783::Komal Arora	3	0	0	3
Course Weightage	ATT: 5 CA: 25 MTT: 20 ETT: 50	**Exam Category: 55: Mid Term Exam: All Subjective – End Term Exam: All Subjective**				
Course Orientation	KNOWLEDGE ENHANCEMENT, RESEARCH					

Course Outcomes :Through this course students should be able to

CO1 :: Describe basics of information security & privacy and step wise implementing controls for it

CO2 :: Apply safeguards to protect the organisation's information resources from theft, abuse, misuse and any form of damage

CO3 :: Apply methods and techniques of activity planning and risk assessment on security projects

CO4 :: Analyze the progress of security project using monitoring and controlling tools

	TextBooks (T)		
Sr No	**Title**	**Author**	**Publisher Name**
T-1	INFORMATION SYSTEMS SECURITY WILEY PUBLICATIONS	NINA GODOLE	WILEY

	Reference Books (R)		
Sr No	**Title**	**Author**	**Publisher Name**
R-1	NETWORK SECURITY: THE COMPLETE REFERENCE ROBERTA: TATAMCGRAW HILL	BRAGG,	MCGRAW HILL EDUCATION
R-2	CRYPTOGRAPHY & NETWORK SECURITY	ATUL KAHATE	MCGRAW HILL EDUCATION

Relevant Websites (RW)		
Sr No	**(Web address) (only if relevant to the course)**	**Salient Features**
RW-1	csc.columbusstate.edu/summers/NOTES/6126/notes/6126-ch3.ppt	program security
RW-2	http://www.infosec.gov.hk/english/technical/files/overview.pdf	security standards
RW-3	https://www.cs.utexas.edu/~byoung/cs361/lecture14.pdf	covert channel
RW-4	http://calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf	information classification
RW-5	www.ijicic.org/ijicic-ksi-13.pdf	biometric systems

An instruction plan is only a tentative plan. The teacher may make some changes in his/her teaching plan. The students are advised to use syllabus for preparation of all examinations. The students are expected to keep themselves updated on the contemporary issues related to the course. Upto 20% of the questions in any examination/Academic tasks can be asked from such issues even if not explicitly mentioned in the instruction plan.

RW-6	csrc.nist.gov/publications/nistbul/Jan2010_securitymetrics.pdf	Security metrics and trusted system
RW-7	http://www2.imm.dtu.dk/courses/02230/lect02.pdf	Computer Security and Information Assurance
RW-8	Security features of Trusted OS	csc.columbusstate.edu/summers/NOTES/6126/notes/6126-ch5.ppt

LTP week distribution: (LTP Weeks)	
Weeks before MTE	7
Weeks After MTE	7
Spill Over (Lecture)	

Detailed Plan For Lectures

Week Number	Lecture Number	Broad Topic(Sub Topic)	Chapters/Sections of Text/reference books	Other Readings, Relevant Websites, Audio Visual Aids, software and Virtual Labs	Lecture Description	Learning Outcomes	Pedagogical Tool Demonstration/ Case Study / Images / animation / ppt etc. Planned	Live Examples
Week 1	Lecture 1	Information Systems (Information system security & threats)	T-1 R-1 R-2		Zero Lecture on Information Security	Student will get to know about the scope and need of the subject	Demonstration	Talk about Wiki Leaks and other security leaks and how the world is affected by it?
	Lecture 2	Information Systems (meaning and importance of information systems)	T-1		L2: Discussion about Meaning and importance of information systems	Student will be more explored about information systems and their use in today world of IT	Demonstration	
	Lecture 3	Information Systems (information security and privacy threat)	T-1		L3: Information security and privacy, discussion about different types of threats	Student will be more explored about information systems and their use in today world of IT	Demonstration	

Week 2	Lecture 4	Building Blocks of Information Security (principles, terms and three pillars of information security)	T-1		L4: Discussion about Principles, Terms, Three Pillars of information security,Information classification: Need and Types L5: Risk Analysis basics, Role of Risk Analysis in Information and Security	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view
		Building Blocks of Information Security(risk management & risk analysis)	T-1		L4: Discussion about Principles, Terms, Three Pillars of information security,Information classification: Need and Types L5: Risk Analysis basics, Role of Risk Analysis in Information and Security	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view
	Lecture 5	Building Blocks of Information Security (principles, terms and three pillars of information security)	T-1		L4: Discussion about Principles, Terms, Three Pillars of information security,Information classification: Need and Types L5: Risk Analysis basics, Role of Risk Analysis in Information and Security	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view
		Building Blocks of Information Security(risk management & risk analysis)	T-1		L4: Discussion about Principles, Terms, Three Pillars of information security,Information classification: Need and Types L5: Risk Analysis basics, Role of Risk Analysis in Information and Security	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view

Week 2	Lecture 6	Building Blocks of Information Security (information classification)	T-1		L6:Risk management and Types: Qualitative and Quantitative Risk Analysis L7: Approaches and Considerations for Risk Analysis and discussion about the effectiveness of these approaches and information classification	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view
		Building Blocks of Information Security (approaches and considerations for risk analysis)	T-1		L6:Risk management and Types: Qualitative and Quantitative Risk Analysis L7: Approaches and Considerations for Risk Analysis and discussion about the effectiveness of these approaches and information classification	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view
Week 3	Lecture 7	Building Blocks of Information Security (information classification)	T-1		L6:Risk management and Types: Qualitative and Quantitative Risk Analysis L7: Approaches and Considerations for Risk Analysis and discussion about the effectiveness of these approaches and information classification	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view

Week 3	Lecture 7	Building Blocks of Information Security (approaches and considerations for risk analysis)	T-1		L6:Risk management and Types: Qualitative and Quantitative Risk Analysis L7: Approaches and Considerations for Risk Analysis and discussion about the effectiveness of these approaches and information classification	Students will learn the importance of various rules associated with information security and privacy along with risk assessment , management and information classification	Demonstration	Demonstration through example about how many factor may lead to another and how whole system can collapse form security point of view
	Lecture 8	Threats(new technologies open door threats)	T-1		L8: Discussion about new technologies, Open Door Threats, Level of Threats,Information Level Threats and Network Level Threats and Attacks	Student will learn about the various threats which we may face any time in any type of I.T. based organization	Discussion	live example of Trojans, worms and viruses
		Threats(level of threats: information, network Level)	T-1		L8: Discussion about new technologies, Open Door Threats, Level of Threats,Information Level Threats and Network Level Threats and Attacks	Student will learn about the various threats which we may face any time in any type of I.T. based organization	Discussion	live example of Trojans, worms and viruses
	Lecture 9	Threats(classifications of threats and assessing damages)	T-1	RW-4	L9: Classification of Threats based on the threat level,Assessing Damages from different types of threats	Student will learn about the various threats which we may face any time in any type of I.T. based organization	Discussion	live example of Trojans, worms and viruses
Week 4	Lecture 10	Program security(overview of program security)		RW-1 RW-7	Outline of Program Security with examples and various programming flaws	Purpose of Defining & Testing secure program and Understanding Taxonomy of program flaws	Discussion	
		Program security(types of flaws)		RW-1 RW-7	Outline of Program Security with examples and various programming flaws	Purpose of Defining & Testing secure program and Understanding Taxonomy of program flaws	Discussion	

An instruction plan is only a tentative plan. The teacher may make some changes in his/her teaching plan. The students are advised to use syllabus for preparation of all examinations. The students are expected to keep themselves updated on the contemporary issues related to the course. Upto 20% of the questions in any examination/Academic tasks can be asked from such issues even if not explicitly mentioned in the instruction plan.

Week 4	Lecture 11	Program security(viruses and other malicious code)		RW-1 RW-7	Study of various viruses and other malicious code	Understanding how Malicious code or rogue pgm is written to exploit flaws in programs	Demonstration	
	Lecture 12	Program security(covert channels)		RW-1 RW-3	L12:Controls against program threats L13:Covert channels	Definition and examples of covert channels and controls against program threats	Discussion	
Week 5	Lecture 13	Program security(controls against program threats)		RW-1 RW-7	L12:Controls against program threats L13:Covert channels	Definition and examples of covert channels and controls against program threats	Discussion	
	Lecture 14	Program security(controls against program threats)		RW-1 RW-7	L12:Controls against program threats L13:Covert channels	Definition and examples of covert channels and controls against program threats	Discussion	
	Lecture 15	Biometrics Controls for Security(access control, user identification & authentication)	T-1	RW-5	L15:Need of access control at different levels L16:Methods for implementing physical access control in organization	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security

Week 5	Lecture 15	Biometrics Controls for Security(biometric techniques)	T-1	RW-5	L15:Need of access control at different levels L16:Methods for implementing physical access control in organization	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security
Week 6	Lecture 16	Biometrics Controls for Security(access control, user identification & authentication)	T-1	RW-5	L15:Need of access control at different levels L16:Methods for implementing physical access control in organization	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security
		Biometrics Controls for Security(biometric techniques)	T-1	RW-5	L15:Need of access control at different levels L16:Methods for implementing physical access control in organization	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security

Week 6	Lecture 17	Biometrics Controls for Security(face recognition and related issues)	T-1	RW-5	L17:Discussion about different biometric techniques for access control and protection L18:Discussion about the corresponding advantages and disadvantages of each biometric access control technique and Limitations of using biometric based access control methods.	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security
		Biometrics Controls for Security(advanced minutiae based algo)	T-1	RW-5	L17:Discussion about different biometric techniques for access control and protection L18:Discussion about the corresponding advantages and disadvantages of each biometric access control technique and Limitations of using biometric based access control methods.	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security
	Lecture 18	Biometrics Controls for Security(face recognition and related issues)	T-1	RW-5	L17:Discussion about different biometric techniques for access control and protection L18:Discussion about the corresponding advantages and disadvantages of each biometric access control technique and Limitations of using biometric based access control methods.	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security

Week 6	Lecture 18	Biometrics Controls for Security(advanced minutiae based algo)	T-1	RW-5	L17:Discussion about different biometric techniques for access control and protection L18:Discussion about the corresponding advantages and disadvantages of each biometric access control technique and Limitations of using biometric based access control methods.	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security
Week 7	Lecture 19	Biometrics Controls for Security(key success factors)		RW-5	L19: Challenges which are faced while implementing biometric based access control methods and Future biometric s	Students will learn about controlling the access at the physical level,User Identification,Authentica tion techniques and need ,The various factors which make biometrics a successful technology in the area of identification and authorizations	Demonstration	Google Data Center Security
		SPILL OVER						
Week 7	Lecture 21				Spill Over			
		MID-TERM						
Week 8	Lecture 22	Security standards and policies(intro to ISO 27001. COBIT, SSE-CMM)	T-1	RW-2	ISO 27001 COBIT,SSECMM Methodologies for Information System Security design and implementation	security models for information protection ISO 27001 COBIT,SSECMM,Met hodologies for Information System Security	Discussion	

Week 8	Lecture 23	Security standards and policies(policies and their elements)	T-1	RW-2	Policy and its role in providing secure IT infrastructure	To understand how Policy and its role in providing secure IT infrastructure	Discussion	
	Lecture 24	Security standards and policies(HIPAA security guidelines)	T-1	RW-2	Security Models and Frameworks related to designing a security oriented infrastructure	Student will get to know about terminology related to security models for information protection	Discussion	
Week 9	Lecture 25	Security standards and policies(methodologies for information system security.: IAM, IEM, SIPES.)	T-1	RW-2	Security Models and Frameworks related to designing a security oriented infrastructure	Student will get to know about terminology related to security models for information protection IAM, IEM, SIPES methodologies for Information System Security,Terminology related to security models for information protection	Discussion	
	Lecture 26	Security standards and policies(methodologies for information system security.: IAM, IEM, SIPES.)	T-1	RW-2	Security Models and Frameworks related to designing a security oriented infrastructure	Student will get to know about terminology related to security models for information protection IAM, IEM, SIPES methodologies for Information System Security,Terminology related to security models for information protection	Discussion	

Week 9	Lecture 27	Security metrics and trusted system(Security matrix)		RW-6	L28: Introduction and discussion about Security matrix Classification L29: Role of security metric in assessing the effectiveness of security infrastructure	Student will get to know about need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
Week 10	Lecture 28	Security metrics and trusted system(Security matrix)		RW-6	L28: Introduction and discussion about Security matrix Classification L29: Role of security metric in assessing the effectiveness of security infrastructure	Student will get to know about need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
		Security metrics and trusted system(Classification)	T-1	RW-6	L28: Introduction and discussion about Security matrix Classification L29: Role of security metric in assessing the effectiveness of security infrastructure	Student will get to know about need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
	Lecture 29	Security metrics and trusted system(Classification)	T-1	RW-6	L28: Introduction and discussion about Security matrix Classification L29: Role of security metric in assessing the effectiveness of security infrastructure	Student will get to know about need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
	Lecture 30	Security metrics and trusted system(Privacy vs security)	T-1		L30: Security Models and standards and discussion about different types of security models. L31: Discussion about the security models	Need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	

Week 10	Lecture 30	Security metrics and trusted system(Security Models)	T-1		L30: Security Models and standards and discussion about different types of security models. L31: Discussion about the security models	Need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
Week 11	Lecture 31	Security metrics and trusted system(Privacy vs security)	T-1		L30: Security Models and standards and discussion about different types of security models. L31: Discussion about the security models	Need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
		Security metrics and trusted system(Security Models)	T-1		L30: Security Models and standards and discussion about different types of security models. L31: Discussion about the security models	Need and basics of security metrics,Classification of security metrics,Privacy concerns with business transactions	Demonstration	
	Lecture 32	Security metrics and trusted system(Trusted OS Design and Principles)		RW-8	Discuss trusted system that incorporate technology to address both features and assurance	Understanding that what makes an operating system “secure” Or “trustworthy"	Demonstration	
	Lecture 33	Security metrics and trusted system(Security features of Trusted OS)		RW-8	L33: Models of Security L34:Trusted OS Design and Security Kernel L35: Trusted Computing Base	Understanding how kernel security is responsible for enforcing security mechanisms of the entire OS and security features of Trusted OS	Discussion	

Week 12	Lecture 34	Security metrics and trusted system(Security features of Trusted OS)		RW-8	L33: Models of Security L34:Trusted OS Design and Security Kernel L35: Trusted Computing Base	Understanding how kernel security is responsible for enforcing security mechanisms of the entire OS and security features of Trusted OS	Discussion	
	Lecture 35	Security metrics and trusted system(Security features of Trusted OS)		RW-8	L33: Models of Security L34:Trusted OS Design and Security Kernel L35: Trusted Computing Base	Understanding how kernel security is responsible for enforcing security mechanisms of the entire OS and security features of Trusted OS	Discussion	
	Lecture 36	Privacy Technological Impacts(Impact of information technology on privacy of an individual)	T-1		Impact of information technology on privacy of an individual and privacy related incidents in the past where individual information was stolen and used inappropriately	Students will learn about the impact of information technology on privacy of an individual, Affect of web technologies on privacy	Demonstration and discussion	
Week 13	Lecture 37	Privacy Technological Impacts(Impact of information technology on privacy of an individual)	T-1		Impact of information technology on privacy of an individual and privacy related incidents in the past where individual information was stolen and used inappropriately	Students will learn about the impact of information technology on privacy of an individual, Affect of web technologies on privacy	Demonstration and discussion	
	Lecture 38	Privacy Technological Impacts(Affect of web technologies on privacy)	T-1 R-1 R-2		Internet related privacy issues and how these can be tackled to protect individual privacy and Discussion about Blackberry and Apple phone related privacy issues	Students will learn about the impact of information technology on privacy of an individual, Affect of web technologies on privacy,	Discussion	

Week 13	Lecture 39	Privacy Technological Impacts(RFID related privacy issues)	T-1 R-1 R-2		Affect of web technologies on privacy and RFID working and privacy related issues	Affect of web technologies on privacy,RFID related privacy issues, Internet related privacy issues	Demonstration	
Week 14	Lecture 40	Privacy Technological Impacts(Internet related privacy issues)	T-1		Internet related privacy issues and how these can be tackled to protect individual privacy	Students will learn about the impact of information technology on privacy of an individual, Affect of web technologies on privacy,	Demonstration	
		SPILL OVER						
Week 14	Lecture 42				Spill Over			
Week 15	Lecture 43				Spill Over			
	Lecture 44				Spill Over			
	Lecture 45				Spill Over			

Scheme for CA:

CA Category of this Course Code is:A0203 (2 best out of 3)

Component	Weightage (%)	Mapped CO(s)
Term paper	50	CO1, CO2, CO3, CO4
Test	50	CO1, CO2
Test - Code based	50	CO3, CO4

Details of Academic Task(s)

Academic Task	Objective	Detail of Academic Task	Nature of Academic Task (group/individuals)	Academic Task Mode	Marks	Allottment / submission Week
Term paper	To give students a team work problem to gather data, conduct research and produce meaningful results.	A topic will be chosen by students and research will be conducted to gain new insights in the field of information security. 30 marks (Mid Term report- 5 marks, End Term report- 15 marks , Viva /presentation- 10 marks)	Individual	Online	30	3 / 12
Test	To test the knowledge of the student related to the subject for CA	The syllabus of test1 will be from lecture 1 to lecture 12. Test will consist of descriptive as well as analytical questions.	Individual	Offline	30	4 / 5
Test - Code based	To check the understanding as well as performance of the students based upon the concepts taught	The syllabus of test2 will be from lecture 13 to lecture 27. Test will consist of descriptive as well as analytical questions	Individual	Offline	30	8 / 10

List of suggested topics for term paper[at least 15] (Student to spend about 15 hrs on any one specified term paper)

Sr. No.	Topic
1	Mobile Devices and Wireless security
2	Black Hat Hacking
3	Trojan Horse
4	Worms
5	Security Audit
6	Spoofing
7	Social Engineering
8	Mobile spoofing
9	Steganography
10	OWASP
11	Network Sniffing
12	BCP
13	DRP
14	Analysis of data packets

An instruction plan is only a tentative plan. The teacher may make some changes in his/her teaching plan. The students are advised to use syllabus for preparation of all examinations. The students are expected to keep themselves updated on the contemporary issues related to the course. Upto 20% of the questions in any examination/Academic tasks can be asked from such issues even if not explicitly mentioned in the instruction plan.

15	Authentication and Authorization
16	DOS and DDOS Attacks