

Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	T	P	L	T	P	Total
MCA5053	Information System Security and Audit	4	-	--	4	-	--	4
		Examination Scheme						
		ISE		MSE		ESE		
		10		30		100 (60% Weightage)		

Pre-requisite Course Codes	Network Security	
Course Outcomes	CO1	To understand the basics of security principles and practices.
	CO2	To analyze data and program security
	CO3	To analyze database and operating system security
	CO4	To understand laws and digital forensic for information security.
	CO5	To analyze security of wireless network and web services
	CO6	To understand security audit.

Module No.	Unit No.	Topics	Ref.	Hrs.
1		Security Principles and Practices		5
	1.1	Information System Security Principles		
	1.2	Threats and Attacks		
	1.3	Classification of threats and assessing damages		
	1.4	Protecting Information Systems Security		
	1.5	Information System Security Engineering Process		
	1.6	Security Policies		
	1.7	standards		
	1.8	Guidelines and Procedures		
2		Data and Program Security		6
	2.1	Data Protection		
	2.2	End Point security,		
	2.3	Physical Security		
	2.4	Insider threats and data Protection Secure programs		
	2.5	Non-malicious program errors		
	2.6	malicious code		
	2.7	Targeted malicious code		
	2.8	Controls against program threats		
3		Operating System Security		5
	3.1	Role of Operating systems in Information systems applications		
	3.2	Operating systems Security		
	3.3	Patched Operating systems		
	3.4	Protected Objects and Methods of Protection		
	3.5	Memory Address Protection		
	3.6	Control of Access to General Objects		
	3.7	File Protection Mechanism		
4		Database Security		5

	4.1	Database Security Requirements and Challenges		
	4.2	Database Integrity, Data Security Policies		
	4.3	Sensitive data		
	4.4	Interface,		
	4.5	Multilevel database Application Software Controls :Concurrency Control		
	4.6	Cryptograph control		
	4.7	Audit train control		
5		Steganography and Digital Forensics		4
	5.1	Steganography- Overview and Principles		
	5.2	need of steganography		
	5.3	pros and cons		
	6.4	Steganography vs Cryptography		
	5.5	Types of Steganography Digital Forensics- Introduction,		
	5.6	Forensic life cycle		
	5.7	Water marking		
6		Laws, & Legal Framework for Information Security		4
	6.1	Introduction, Information Security and Law		
	6.2	Understanding the Laws of Information Security		
	6.3	Indian IT Act, Laws of IPR		
	6.4	Patent laws		
	6.5	Copyright Law		
	6.6	Ethical Issues in Information Security: Introduction		
	6.7	Issues in Network enterprises,		
	6.8	Computer Ethics and Security and Privacy Policies		
7		Software Web Services Security		4
	7.1	Technologies for web services (XML, SOAP, WSDL & UDDI)		
	7.2	Web Services Security – Token types,		
	7.3	XML encryption		
8		Security of Wireless Networks		4
	8.1	An overview of wireless technology		
	8.2	Wired world versus wireless world: putting Wireless Networks in Information Security Context,		
	8.3	Attacks on Wireless Networks		
9		Auditing for Security		8
	9.1	Introduction		
	9.2	Organizations Roles and Responsibilities for Security Audits		
	9.3	Auditors Responsibilities for Security Audits,		
	9.4	Types of Security Audits		
	9.5	Technology Based Audits		
	9.6	Phases in Security Audits		
	9.7	Budgeting for Security Audits		
			Total	45

References :

- [1] Nina Godbole, “Information Systems Security”, Wiley India
- [2] Eric Cole, “Network Security Bible”, Wiley India Edition
- [3] C. P. Pfleeger, and S. L. Pfleeger, “Security in Computing”, Pearson Education.