Course Code	Course Title	L	T	P	C
OLMCA622	Information Security	3	1	0	4
Pre-requisite	NIL	Syllabus Version			
		1.0			

Course Objectives

1. Understand the fundamentals of information security and audit.
2. Identify and analyze information security threats, attacks and counter measures.
3. Develop skills in understanding information assurance, Incident management and response.
4. Understand the importance of security audit.

Course Outcome

At the end of the course the student will be able to

1. Explain the core principles of information security.
2. Identify major information security threats and attacks.
3. Describe network security methods including firewalls, honeypots.
4. Explain intrusion detection systems (IDS) and intrusion prevention systems (IPS), outlining their pros and cons.
5. Coordinate responses to information security incidents
6. Contribute to information security audits

Module:1	Introduction to Information Security

Evolution of Information Security – Confidentiality , Integrity, Authentication – The CIA Triad – Security Framework – Information Assets – Identity and Access management – Access Control Structures - Access management tools.

Module:2	Threats and Attacks

Overview of Threats - Understanding Threats, Attacks, Vulnerabilities and Risks - Types of attacks – Malware attacks- Phishing attacks - IP Spoofing attacks – Password attacks – Denial of Service and Distributed Denial of Service attacks - Social Engineering attacks.

Module:3	System and Network Security

System Vulnerabilities and Mitigations – System Security Tools – Network security solutions – Firewalls – Design and Principles - Types of Firewalls – Packet Filtering Firewall – Stateful Inspection Firewall – Proxy Firewall - Honey pots – Trusted Systems.

Module:4	Intrusion Detection and Prevention

Intrusion Detection – Signature Based Intrusion Detection - Anomaly based Intrusion Detection – Rule based Intrusion Detection – Network based Intrusion Detection – Host based Intrusion Detection – Intrusion Prevention System

Module:5	Information Assurance Management

System Monitoring and Control - Automated Security Assessments - Backup Strategies for Security Devices - Performance Evaluation - Information Security Governance Framework – Policies, Procedures, Standards and Guidelines

Module:6	Incident Management and Response

Risk Management - Risk Assessment - Security incident management – Incident – Components and Roles – Incident Response Life cycle – Incident Analysis.

Module:7	Information Security Audit

Nature and Scope - Security audit – Roles and Responsibilities – Identify the requirements, policies, guidelines in auditing – Vulnerability Assessment – Penetration testing – Ethics of Information Security auditor.				
		Total Hours of Study:		**120**
Text Book(s)				
1.	Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wiley, 2017			
Reference Books				
1.	William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd edition, 2014			
2.	Andrew Vladimirov Michajlowski, Konstantin, Gavrilenko, Assessing Information Security: Strategies, Tactics, Logic and Framework, IT Governance Ltd, O'Reilly, 2010			
Mode of Evaluation: CAT / written assignment / Quiz / FAT / Project / Seminar / group				
Recommended by Board of Studies		28-10-2024		
Approved by Academic Council		No. 76	Date	28-11-2024