CSE3502	Information Security Management	L	T	P	J	C
		2	0	2	4	4
Pre-requisite	NIL	**Syllabus version**				
		1.0				

Objective of the course

1. To introduce system security related incidents and insight on potential defenses, counter measures against common threat/vulnerabilities.
2. To provide the knowledge of installation, configuration and troubleshooting of information security devices.
3. To make students familiarize on the tools and common processes in information security audits and analysis of compromised systems.

Expected Outcome

After successfully completing the course the student should be able to

1. Contribute to managing information security
2. Co-ordinate responses to information security incidents
3. Contribute to information security audits
4. Support teams to prepare for and undergo information security audits
5. Maintain a healthy, safe and secure working environment
6. Provide data/information in standard formats
7. Develop knowledge, skills and competence in information security

Student Learning Outcomes (SLO)	**1, 2, 17**

1. Having an ability to apply mathematics and science in engineering applications
2. Having a clear understanding of the subject related concepts and of contemporary issues
17. Having an ability to use techniques, skills and modern engineering tools necessary for engineering practice

1	**Information Security Devices**	5 hours

Identify And Access Management (IdAM), Networks (Wired And Wireless) Devices, Endpoints/Edge Devices, Storage Devices, Servers, Infrastructure Devices (e.g. Routers, Firewall Services) , Computer Assets, Servers And Storage Networks, Content management, IDS/IPS

2	**Security Device Management**	6 hours

Different types of information security devices and their functions,
Technical and configuration specifications, architecture concepts and design patterns and how these contribute to the security of design and devices.

3	**Device Configuration**	5 hours

Common issues in installing or configuring information security devices, Methods to resolve these issues, Methods of testing installed/configured information security devices,

4	**Information Security Audit Preparation**	5 hours

Establish the nature and scope of information security audits, Roles and responsibilities, Identify the procedures/guidelines/checklists, Identify the requirements of information security, audits and prepare for audits in advance, Liaise with appropriate people to gather data/information required for information security audits. **Security Audit Review -**
Organize data/information required for information security audits using standard templates and tools, Audit tasks, Reviews, Comply with the organization's policies, standards, procedures, guidelines and checklists, Disaster Recovery Plan

5	**Team Work and Communication**	2 hours
Communicate with colleagues clearly, concisely and accurately , Work with colleagues to integrate their work effectively, Pass on essential information to colleagues in line with organizational requirements, Identify any problems they have working with colleagues and take the initiative to solve these problems, Follow the organization's policies and procedures for working with colleagues		
6	**Managing Health and Safety**	2 hours
Comply with organization's current health, safety and security policies and procedures, Report any identified breaches in health, safety, and Security policies and procedures, Identify, report and correct any hazards, Organization's emergency procedures, Identify and recommend opportunities for improving health, safety, and security.		
7	**Data and Information Management**	3 hours
Fetching the data/information from reliable sources, Checking that the data/information is accurate, complete and up-to-date, Rule-based analysis of the data/information, Insert the data/information into the agreed formats, Reporting unresolved anomalies in the data/information.		
8	**Learning and Self Development**	2 hours
Identify accurately the knowledge and skills needed, Current level of knowledge, skills and competence and any learning and development needs, Plan of learning and development activities to address learning needs, Feedback from appropriate people, Review of knowledge, skills and competence regularly and appropriate action taken		

	Total Lecture hours:	**30 hours**

Text Book(s)

1. Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Nina Godbole, Wiley, 2017
2. Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition, . Information Security Management: Concepts and Practice. New York, McGraw-Hill, 2013.
3. Christopher J. Alberts, Audrey J. Dorofee , Managing Information Security Risks, Addison-Wesley Professional, 2004

Reference Books

1. Andrew Vladimirov Michajlowski, Konstantin, Andrew A. Vladimirov, Konstantin V. Gavrilenko, Assessing Information Security: Strategies, Tactics, Logic and Framework, IT Governance Ltd, O'Reilly 2010
2. Christopher J. Alberts, Audrey J. Dorofee , Managing Information Security Risks, Addison-Wesley Professional, 2004
3. Chuck Easttom , System Forensics Investigation and Response, Second Edition, Jones & Bartlett Learning, 2014
4. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, Metasploit The
5. Penetration Tester's Guide, No Starch Press, 2014

Ref Links:
https://www.iso.org/isoiec-27001-information-security.html
https://www.sans.org/reading-room/whitepapers/threats/paper/34180
https://csrc.nist.gov/publications/detail/sp/800-40/version-20/archive/2005-11-16
https://www.sscnasscom.com/qualification-pack/SSC/Q0901/

List of Experiments (Indicative)		SLO: 1,2,17
1.	• Install and configure information security devices • Penetration Testing • MySQL SQL Injection • Information security incident Management • Intrusion Detection/Prevention • Port Redirection and Tunneling • Exploring the Metasploit Framework • Working with Commercial Tools like HP Web Inspect and IBM AppScan etc., • Explore Open Source tools like sqlmap, Nessus, Nmap etc • Documentation with Security Templates from ITIL • Carry out backups of security devices and applications in line with information security policies, procedures and guidelines • Information security audit Tasks - Procedures/guidelines/checklists for the audit tasks	
	Total Laboratory Hours	**30 hours**

Recommended by Board of Studies	05.02.2020		
Approved by Academic Council	58	Date	26.02.2020