Course Code	Course Title	L	T	P	C
BCSE354E	Information Security Management	1	0	2	2
Pre-requisite	NIL	Syllabus version			
		1.0			

Course Objectives

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

Course Outcomes

1. Understand and manage information security Devices
2. Configure and install information security devices
3. Organize a healthy, safe and secure working environment
4. Interpret the data/information in standard formats
5. Develop knowledge, skills and competence in information security

Module:1	Information Security Devices	2 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.

Module:2	Security Device Management	2 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.

Module:3	Device Configuration	2 hours

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

Module:4	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.

Module:5	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.

Module:6	Data and Information Management	2 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.		
Module:7	**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.		
Module:8	**Contemporary Issues**	**1 hour**
	Total Lecture hours:	**15 hours**

Text Book(s)	
1.	Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition,. Information Security Management: Concepts and Practice. New York, McGraw-Hill, 2013.
2.	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 Penetration Tester's Guide, No Starch Press, 2014.
5.	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/

Mode of Evaluation: CAT, Quiz and FAT		
Indicative Experiments		
1.	Install and configure information security devices	
2.	Penetration Testing	
3.	MySQL SQL Injection	
4.	Intrusion Detection/Prevention	
5.	Port Redirection and Tunneling	
6.	Working with Commercial Tools like HP Web Inspect and IBM AppScan etc.,	
7.	Explore Open Source tools like sqlmap, Nessus, Nmap etc	
	Total Laboratory Hours	**30 hours**
Mode of assessment: CAT / FAT		

Recommended by Board of Studies	DD-MM-YYYY		
Approved by Academic Council		Date	