T. Y. B. Tech (Computer Science and Engineering) Sem – VI

5. Open Elective Course - II (OEC - CS606)

Cyber Security (OEC - CS606)

TEACHING SCHEME	EXAMINATION SCHEME
Theory : 3 Hrs./Week	**Theory :** ESE 70 Marks CIE 30 Marks
Tutorial : -----	**Term work : -----**
Practical : -----	**Practical : -----**

Prerequisite: Fundamental knowledge of Data Communication, Networking and Information Security.

Course Objectives:

1. To gain knowledge about securing both clean and corrupted systems, protect personal data, and secure computer networks

2. To examine secure software development practice

3. To understand key terms and concepts in I.T. ACT

4. To incorporate approaches for incident analysis and response

Course Outcomes:

On completion of the course, student will be able to

1. Explain the cyber security concepts.

2. Describe the cyber security vulnerabilities and prevention techniques.

3. Explain the different rules and regulations under I.T. ACT.

4. Explain the concepts of digital forensics & incident management

UNIT NO.	UNIT NAME & DETAILS	NO. OF LECTURES
1.	**Computer and Network Security** Introduction to Computer Security - Introduction, How Seriously Should You Take Threats to Network Security?, Identifying Types of Threats, Basic Security Terminology, Concepts and Approaches, Online Security Resources Networks and the Internet : Introduction, Network Basics, How the Internet Works, Basic Network Utilities , Advanced Network Communications Topics	06
2.	**Cyber Frauds, DoS, Viruses:** Cyber Stalking, Fraud, and Abuse: Introduction, How Internet Fraud Works, Identity Theft, Cyber Stalking, Protecting Yourself	06

	Against Cyber Crime. Denial of Service Attacks: Introduction, DoS, Illustrating an Attack, Malware: Introduction, Viruses, Trojan Horses, The Buffer-Overflow Attack. The Sassier Virus/Buffer Overflow, Spyware, Other Forms of Malware, Detecting and Eliminating Viruses and Spyware	
3.	**Techniques Used by Hackers :** Introduction, Basic Terminology, The Reconnaissance Phase, Actual Attacks, Malware Creation, Penetration Testing	**06**
4.	**Computer Security Technology:** Introduction, Virus Scanners, Firewalls, Antispyware, IDS, Digital Certificates, SSL/TLS, Virtual Private Networks, Wi-Fi Security	**06**
5.	**I.T. ACT:** Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, I.T. Act	**06**
6.	**Introduction to Forensics:** Introduction, General Guidelines, Finding Evidence on the PC, Finding Evidence in System Logs , Getting Back Deleted Files, Operating System Utilities, Operating System Utilities, Mobile Forensics: Cell Phone Concepts	**06**

Text Books:

1. Computer Security Fundamentals - Chuck Easttom, Pearson, third edition.

Reference Books:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Osborne Media, 3 rd edition , 2014.
2. Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005.
3. John Sammons, the Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Paperback, February 24, 2012.
4. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George.Kurtz, McGraw-Hill, 2005.
5. Ethical Hacking, Thomas Mathew, OSB Publisher, 2003.
7. Dave Shackleford, Virtualization Security: Protecting Virtualized Environments, John Wiley & Sons, 2012.
8. BRAGG, Network Security: The Complete Reference, McGraw Hill Professional, 2012