Subject Code	Subject Name	Period/Week		Credit
28573	Cyber Security & Ethics	T	P	C
		2	3	3

Rationale	This is an occupational-specific subject in the curriculum for diploma in engineering courses required to enable the graduate to use and work with Cyber security field which is very essential for an IT professional. This course enhances the students' knowledge & skills on Cyber security fields and also help to provide job placement or self-employment of the students.
Learning Outcome (Theoretical)	**After completing the theoretical course, students should be able to:** • interpret types and methodology of Cyber security & Risk management, importance of Cyber Security Laws & rules • illustrate of computer & Internet security, security resources, security tools, types of Firewall, types of threat & attack and securing data storage system • explain details of Vulnerability Assessment, Penetration Testing • describe basic of Blockchain technology, Data Security and Digital Forensics • explain about Incidents Response and Disaster Recovery • illustrate basics of IT Security Auditing
Learning Outcome (Practical)	**After completing the practical course, students should be able to:** • apply network security, system security and basic data security • perform the techniques of exploit vulnerabilities and techniques of post exploitation of vulnerabilities • apply data hiding techniques using Steganography and Cryptography techniques • apply application data security • perform system forensics, mobile and IoT forensics • prepare forensic report • apply the Governance and Management of IT audit

Detailed Syllabus (Theory)

Unit	Topics with Contents	Period	Marks
1	**Cyber Security and Risk Management** 1.1 Define cyber security & goal of cyber security 1.2 Interpret cyber security & risk management 1.3 Explain structure of cyber world 1.4 Illustrate type of cyber security 1.5 Explain functional framework of cyber security 1.6 Describe risk management framework 1.7 Illustrate basic risk analysis methodology & risk mitigation process 1.8 Illustrate ethical hacking 1.9 Interpret importance of cyber security laws & rules 1.10 Explain user awareness and training for cyber security	**3**	**10**
2	**System and Network Security** 2.1 State system and network security 2.2 Describe computer, network & internet security resources 2.3 Explain the use of security tools 2.4 Define firewall & state the types of firewall 2.5 Define threat and mention types of threat 2.6 Illustrate wireless attack & attacks on different layer 2.7 Illustrate basic data security and securing data storage system	**3**	**8**
3	**Vulnerability Assessment and Penetration Testing** 3.1 Define vulnerability assessment and penetration testing (VAPT) 3.2 Describe types of vulnerability scanning & penetration testing 3.3 explain penetration testing phases and techniques 3.4 Illustrate wireless hacking and different types of hacking tools 3.5 Explain log files and command & control Centre (CnC) 3.6 State VAPT report	**4**	**10**
4	**Data Security** 4.1 Define data security, database security and data privacy 4.2 Illustrate different types of steganography 4.3 Describe various data hiding techniques 4.4 Explain steganography and steganography algorithms 4.5 Explain data encryption algorithms and techniques 4.6 Explain encrypted data storage technique is used in databases 4.7 Illustrate digital signatures and digital certificates techniques	**5**	**8**
5	**Blockchain Technology** 5.1 State blockchain & blockchain technology 5.2 Mention application field of blockchain technology 5.3 Explain blockchain mining process **5.4** Describe blockchain security techniques	**3**	**5**
6	**Digital Forensics** 6.1 Define digital crime 6.2 Mention the classification of digital crime	**6**	**8**

	6.3 Illustrate digital forensic and digital forensic investigation processes 6.4 State the type of file system and file carving techniques 6.5 Describe the techniques of network log forensic, cloud forensic techniques, database forensic techniques, network log forensic technique, cloud forensic techniques, malware forensic and mobile forensic. 6.6 Explain defeating anti-forensic techniques is applied. 6.7 Describe forensic investigation report		
7	**Incidents Response and Disaster Recovery** 7.1 Define incident handling and disaster recovery 7.2 Describe the classification of incident elements handling process 7.3 Explain phases of incident handling 7.4 Illustrate disaster recovery strategy and policy 7.5 Explain steps of disaster recovery	**4**	**6**
8	**IT Security Auditing** 8.1 Define it audit 8.2 Describe types of it audit 8.3 Explain the process of auditing information systems 8.4 Explain the processes of it auditing 8.5 Explain it audit sampling methodology 8.6 Describe it audit reporting process	**4**	**5**
	Total	**32**	**60**

Detailed Syllabus (Practical)

Sl.	Experiment name with procedure	Class (3 Period)	Marks
1	**Apply network security** 1.1 Identify Network security tools as per requirement 1.2 Implement the Network firewall configuration as per job sheet 1.3 Apply Wireless security as per Job Sheet of course Instructor 1.4 Submit records to the course instructor.	1	5
2	**Apply system security** 2.1 Identify System security tools as per requirement 2.2 Apply the System hardening as per instruction sheet (supplied by the course instructor) 2.3 Apply basic System commands for system security as per instruction sheet of instructor 2.4 Apply Host based security as per Job sheet 2.5 Implement the System firewall configuration as per job sheet 2.6 Submit records to the course instructor	1	5
3	**Apply basic data security** 3.1 Identify basic data security & data encryption tools as per requirement 3.2 Implement Strong password mechanism for data security 3.3 Apply Data Encryption using encryption tools	1	4

	3.4 Submit records to the course instructor		
4	**Apply the techniques of exploit vulnerabilities** 4.1 Identify basic System hacking tools as per requirement 4.2 Apply System hacking tools as per instruction sheet 4.3 Use Sniffing tools as per instruction sheet 4.4 Use Malware analysis tools as per instruction sheet 4.5 Apply Wireless hacking tools as per instruction sheet 4.6 Use Mobile device / platform hacking tools as per instruction sheet 4.7 Use Web server and web application hacking tools as per instruction sheet	2	4
5	**Perform the techniques of post exploitation of vulnerabilities** 5.1 Review the Vulnerabilities assessment 5.2 Perform disabling protections 5.3 Apply Local vulnerabilities Assessment 5.4 Perform creation and Leveraging of Backdoors 5.5 Manage Log files 5.6 Apply Data search and extraction techniques 5.7 Generate VAPT Report	3	4
6	**Apply data hiding techniques using Steganography** 6.1 Identify Steganography detecting tools as per requirement 6.2 Apply Streaming media 6.3 Apply multilingual steganography	1	4
7	**Apply Cryptography techniques** 7.1 Identify required tools as per job sheet supplied by the course instructor 7.2 Use Digital signatures and digital certificates techniques 7.3 Apply Cryptosystems as per instruction sheet 7.4 Use Hash functions as per requirement	1	4
8	**Apply application data security** 8.1 Identify required tools as per job sheet supplied by the course instructor 8.2 Use Encrypted data storage technique in databases. 8.3 Rectify SQL and Code injection attacks 8.4 Apply Encrypted network protocols for data security.	1	4
9	**Perform system forensics** 9.1 Identify required tools as per job sheet supplied by the course instructor 9.2 Perform Network log forensic technique 9.3 Perform Cloud forensic techniques and database forensic techniques are performed. 9.4 Apply Malware forensic technique 9.5 Apply Defeating anti-forensic techniques 9.6 Perform Operating system forensics	2	4
10	**Perform mobile and IoT forensics** 10.1 Identify required tools as per job sheet supplied by the course	1	4

	instructor 10.2 Apply Mobile forensic process is defined. 10.3 Perform IoT forensic on IoT devices		
11	**Prepare forensic report** 11.1 Identify required tools as per job sheet supplied by the course instructor 11.2 Prepare Forensic investigation report template 11.3 Prepare Chain-of-Custody document 11.4 Prepare Expert witness report 11.5 Maintain Legal procedure 11.6 Prepare final report	1	4
12	**Apply the Governance and Management of IT audit** 12.1 Identify required tools as per job sheet supplied by the course instructor 12.2 Perform Business Impact Analysis (BIA) 12.3 Prepare Business Continuity Plan (BCP) 12.4 Performed IT Audit according to IT governance and management practices	1	4
	Total	16	50

Necessary Resources (Tools, equipment's and Machinery):

Sl	Item Name	Quantity
01	Desktop PC	25 nos
02	Internet connection	At least 20Mbps

Recommended Books:

Sl	Book Name	Writer Name	Publisher Name & Edition
01	Cybersecurity Ethics and Introduction	By Mary Manjikian	1st Edition
02	The Ethics of Cybersecurity	Christen, Markus (editor) Gordijn, Bert (editor) Loi, Michele (editor)	
03	Cybersecurity, Ethics, and Collective Responsibility	Seumas Miller and Terry Bossomaier	

Website References:

Sl	Web Link	Remarks
01	**http://library.oapen.org/handle/20.500.12657/22489**	
02	**https://www.ollusa.edu/blog/cybersecurity-ethics.html**	