Lok Jagruti Kendra University
University with a Difference

Diploma in Cloud Computing & Big Data

LJ Polytechnic

Course Code: 025100607

Fundamentals of Cyber Security

Programme / Branch Name			Diploma in Cloud Computing & Big Data			
Course Name	Fundamentals of Cyber Security				**Course Code**	025100607
Course Type	HSSC	BSC	ESC	PCC	OEC	PEC

Legends: HSSC: Humanities and Social Sciences Courses BSC: Basic Science Courses
ESC: Engineering Science Courses PCC: Program Core Courses
OEC: Open Elective Courses PEC: Program Elective Courses

1. Teaching and Evaluation Scheme

Teaching Hours / Week / Credits				**Evaluation Scheme**			
L	**T**	**P**	**Total Credit**	**CCE**	**SEE (Th)**	**SEE (Pr)**	**TOTAL**
3	0	4	5	50	50	50	150

Legends:
L: Lectures T: Tutorial P: Practical
CCE: Continuous & Comprehensive Evaluation
SEE (Th): Semester End Evaluation (Theory)
SEE (Pr): Semester End Evaluation (Practical)

2. Prerequisites

- ✓ Basic computer networking
- ✓ Data Communication Technologies
- ✓ Concepts of network and email security

3. Rationale

This course provides the foundation for understanding the key issues associated with protecting information assets. The purpose of the course is to provide the student with an overview of the field of information security and assurance. In this digital age, the information and data are immense and need to be secured.

4. Objectives

- ✓ Identifying the Cyber hacker types
- ✓ Learning to examine the Cyber-attack patterns and provide security measures for them
- ✓ Learn the Cyber laws formed to effectively act upon Cyber crimes

5. Contents

Unit No.	Topics	Sub-Topic	Learning Outcomes	% Weightage	Hours
1	**Fundamentals of Cyber Security**	1.1 Introduction to Cyber Security 1.2 Importance and Challenges in Cyber Security 1.3 Cyberspace 1.4 Cyber Threats 1.5 Cyber Warfare 1.6 CIA Triad 1.7 Cyber Terrorism 1.8 Cyber Security of Critical Infrastructure 1.9 Cyber Security 1.10 Organizational Implications	• To understand fundamentals of Cyber Security and its importance. • To Understand the Cyberspace, Cyber threats, Cyber warfare, and the CIA triad • To Understand the Cyber Security of critical infrastructure and the organizational implications • To identify strategies for dealing with Cyber Security threats and challenges.	15	7
2	**Hackers and Cyber Crimes**	2.1 Types of Hackers 2.2 Hackers and Crackers 2.3 Cyber-Attacks and Vulnerabilities 2.4 Malware Threats 2.5 Sniffing 2.6 Gaining Access 2.7 Escalating Privileges 2.8 Executing Applications 2.9 Hiding Files 2.10 Covering Tracks 2.11 Worms 2.12 Trojans 2.13 Viruses 2.14 Backdoors	• To learn about the different types of hackers • Understand the various Cyber-attacks and how to protect against them. • Identify vulnerabilities in systems and mitigate them. • Understand the various types of malware and how to protect against them. • Learn about different methods used by hackers to gain access to systems. • Understand how hackers can escalate privileges and execute applications.	25	10

			• Learn about hiding files, Covering tracks, and other malicious activities. • Become aware of worms, trojans, and viruses and how to prevent them. • Learn about backdoors and how to prevent them.		
3	**Ethical Hacking and Social Engineering**	3.1 Ethical Hacking Concepts and Scopes 3.2 Threats and Attack Vectors 3.3 Information Assurance 3.4 Threat Modeling 3.5 Enterprise Information Security Architecture 3.6 Vulnerability Assessment and Penetration Testing 3.7 Types of Social Engineering 3.8 Insider Attack 3.9 Preventing Insider Threats 3.10 Social Engineering Targets and Defense Strategies.	• Understand the concept of ethical hacking and the different scopes and approaches to it. • Identify different types of threats and attack vectors. • Learn about information assurance and how to protect data and systems from unauthorized access. • Develop a threat modeling strategy to assess security vulnerabilities and develop countermeasures. • Learn about enterprise information security architecture and best practices for implementation. • Understand the different types of penetration testing and the techniques used. • Be aware of the different types of social engineering and their potential risks.	20	9

			• Understand the concept of insider threats and how to prevent them. • Learn social engineering targets and defense strategies to protect against these attacks.		
4	**Cyber Forensics and Auditing**	4.1 Introduction to Cyber Forensics 4.2 Computer Equipment and Associated Storage Media 4.3 Role of Forensics Investigator 4.4 Forensics Investigation Process 4.5 Collecting Network Based Evidence 4.6 Writing Computer Forensics Reports 4.7 Auditing 4.8 Plan an Audit Against A Set of Audit Criteria	• Demonstrate an understanding of the fundamentals of Cyber forensics. • Comprehend the role of a forensics investigator. • Identify and implement the steps of the forensics investigation process. • Develop the ability to collect network based evidence. • Write a comprehensive computer forensics report. • Develop skills in data auditing and planning an audit against a set of audit criteria.	25	9
5	**Cyber Ethics and Laws**	5.1 Introduction to Cyber Laws 5.2 E-Commerce And E-Governance 5.3 Certifying Authority and Controller 5.4 Offences Under IT Act 5.5 Computer Offences and Its Penalty Under IT Act 2000	• Understand the fundamentals of Cyber laws, their relevance and application in the digital world. • Learn about the latest developments in E-commerce and E-governance. • Gain insight into the roles of certifying authorities and controllers. • Develop knowledge of the offences under the	15	7

		5.6 Intellectual Property Rights in Cyberspace.	IT Act and the penalties associated with them. • Develop an understanding of intellectual property rights in Cyberspace.		
				Total Hours	**42**

6. List of Practicals / Exercises

The practical/exercises should be properly designed and implemented in an attempt to develop different types of skills so that students can acquire the competencies/programme outcomes. Following is the list of practical exercises for guidance.

Sr. No.	Practical / Exercises	Key Competency	Hours
1	Study of different wireless network components and features of any one of the Mobile Security Apps.	To learn about the kinds of security works on system	4
2	Study of the features of Firewall in providing network security and to set Firewall Security in Windows.	To learn about the kinds of security application on System	4
3	Steps to ensure security of any one web browser (Mozilla Firefox/Google Chrome)	To learn about security of web browser	4
4	Study of different types of vulnerabilities for hacking a websites / web application.	To learn about the kind of attacks on websites and web applications	4
5	Analysis the Security Vulnerabilities of E-commerce services.	To learn about the kinds of attacks on E-commerce websites	4
6	Analysis of the security vulnerabilities of E-Mail application	To learn about the kinds of attacks on E-mail applications and how to be aware of the attacks	4
7	Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding Cyber-attack/vulnerability.	To learn about how to install Kali Linux operating system and to use tools for Cyber attack	4
8	Evaluate network defense tools for following: (i) IP spoofing (ii) DOS attack	To learn about working of IP spoofing and DOS attack	4
9	Explore the Nmap tool and list how it can be used for network defense and also explore the NetCat tool	To learn about working of NMAP and NetCat Tools	4
10	Use Wireshark tool and explore the packet format and content at each OSI layer.	To learn about working of Wireshark Tools	4

11	Examine SQL injection attack.	To learn about working of SQL injection attack	4
12	Examine software key loggers and hardware key loggers.	To learn about working of software key loggers and hardware key loggers	4
13	Perform online attacks and offline attacks of password cracking.	To learn about online attacks and offline attacks of password cracking	4
14	Consider a case study of Cyber-crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker	To learn about Cyber laws on the given case	4
		Total Hours	**56**

7. Suggested specification Table with hours

Unit No.	Chapter Name	Teaching Hours	Distribution of Topics According to Bloom's Taxonomy					
			R %	U %	App %	C %	E %	An %
1	Fundamentals to Cyber Security	7	40	30	20	-	5	5
2	Hackers and Cyber Crimes	10	30	30	20	-	10	10
3	Ethical Hacking and Social Engineering	9	20	30	30	10	5	5
4	Cyber Forensics and Auditing	9	20	25	20	-	15	20
5	Cyber Ethics and Laws	7	20	20	30	-	15	15

Legends: R: Remembering U: Understanding
App: Applying C: Creating
E: Evaluating An: Analyzing

8. Text Books

1) "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives" by Nina Godbole and Sunit Belpure, Publication Wiley

9. Reference Books

1) "Enterprise Cyber Security -How to Build a Successful Cyber defense Program against Advanced Threats", Donaldson, S. Siegel, S. Williams, C.K., Aslam, Apress, 1st Edition, 2015.
2) "Hacking the Hacker", Roger Grimes, Wiley, 1st Edition, 2017.
3) "Cyber Security and Cyber Laws Paperback – 2018 " by Alfred Basta, Nadine Basta , Mary Brown , Ravinder Kumar, publication Cengage
4) "Anti-Hacker Tool Kit (Indian Edition)" by Mike Shema, Publication Mc Graw Hill
5) "Cyber Security and laws – An Introduction", Madhumita Chaterjee, Sangita Chaudhary, Gaurav Sharma, Staredu Solutions

10. Open Sources (Website, Video, Movie)

1) https://www.simplilearn.com/learn-Cyber-security-basics-skillup
2) https://www.mygreatlearning.com/academy/learn-for-free/courses/introduction-to-Cyber-security
3) https://www.youtube.com/watch?v=lZl2qWc3vUQ
4) https://onlinecourses.swayam2.ac.in/cec23_cs03/preview
5) https://www.oxfordhomestudy.com/courses/Cyber-security-courses/free-Cyber-security-training