

**PROGRAMME PROJECT REPORT
OF
DIPLOMA IN CYBER SECURITY
(ODL/ONLINE MODE)**

**ONE YEAR (TWO SEMESTER) PROGRAMME
(Effective from Session 2025-26)**



**CENTRE FOR DISTANCE AND
ONLINE EDUCATION**

**GURU JAMBHESHWAR UNIVERSITY OF SCIENCE
AND TECHNOLOGY HISAR-125001, HARYANA**

(YEAR:2025-26)

PROGRAMME PROJECT REPORT (PPR)

DIPLOMA IN CYBER SECURITY

1. PROGRAMME'S MISSION & OBJECTIVE

1.1 PROGRAMME MISSION:

The mission of the Diploma in Cyber Security programme is to equip students with the essential knowledge, practical skills, and ethical foundation needed to protect information systems and digital assets in an increasingly interconnected world. The programme aims to develop competent professionals who can identify, analyze, and mitigate cyber threats across various platforms and environments.

This diploma is designed to provide a strong foundation in core areas such as network security, cryptography, ethical hacking, digital forensics, and cyber law. It focuses on hands-on training, enabling students to apply theoretical knowledge to real-world security challenges. The programme also emphasizes critical thinking, problem-solving, and continual learning to adapt to the rapidly evolving cyber threat landscape.

A key goal is to install a strong sense of professional ethics, responsibility, and awareness of legal and regulatory issues related to cyber security. Graduates of the programme will be prepared to contribute effectively to organizational security frameworks, support national cyber defense efforts, and promote safe digital practices.

Ultimately, the mission of the Diploma in Cyber Security is to create skilled, responsible, and industry-ready cyber security professionals who can ensure the confidentiality, integrity, and availability of digital information in various sectors.

1.2 PROGRAMME OBJECTIVES:

- **Provide Fundamental Knowledge:** To impart a strong foundation in cyber security principles, practices, and tools.
- **Develop Practical Skills:** To equip students with hands-on skills in ethical hacking, network defense, and cyber threat analysis.
- **Ensure Technical Competence:** To enable students to secure computer systems, networks, and data against cyber-attacks.
- **Promote Cyber Ethics and Legal Awareness:** To foster understanding of cyber laws, data privacy regulations, and ethical responsibilities.



- **Enhance Problem-Solving Abilities:** To develop analytical thinking and troubleshooting skills for managing cyber security incidents.
- **Prepare for Industry Requirements:** To align student skills with current industry needs and prepare them for entry-level cyber security roles.
- **Encourage Research and Innovation:** To promote curiosity, research, and innovation in addressing emerging cyber security challenges.
- **Develop Communication and Teamwork Skills:** To enhance collaboration and reporting abilities essential for working in cyber security teams.
- **Support Lifelong Learning:** To instill a habit of continuous learning to keep up with evolving technologies and threats.
- **Contribute to National and Organizational Security:** To prepare professionals capable of supporting cyber defense at both organizational and national levels.

2. RELEVANCE OF THE PROGRAMME WITH HIGHER EDUCATIONAL INSTITUTION'S (HEI'S) MISSION & GOALS

2.1 HEI'S MISSION:

The University aspires to be a globally recognized Centre of excellence in the field of technical education and research. It strives to achieve this by introducing innovative job-oriented courses, employing competent and motivated faculty, developing state-of-the-art infrastructure, striking purposeful linkages with industry and professional bodies, and promoting quality of work life on campus. The University focuses on the student community to imbue them with passion for knowledge and creativity and to promote sustainable growth in academic resources, student placements, and holistic human development with a strong conviction for professional ethical, social and environmental issues.

2.2 HEI's GOALS

The goals of the University as enshrined in the Act are to facilitate and promote studies and research in emerging areas of higher education with focus on new frontiers of and also to achieve excellence in these and connected fields.

2.3 PROGRAMMES OFFERED TO ACHIEVE HEI'S MISSION AND GOALS

The HEI's mission and goals are holistically inherited in the Diploma in Cyber Security of Centre for Distance & Online Education. The Scheme and syllabus of this programme is



designed by Board of Studies and the same is approved by Academic Council. Latest and updated curriculum is used to meet the Cyber Security. This programme focuses primarily on Cyber Security which is an amalgamation of computer sciences, and technologies that has become one of the most prominent applications of technology in the world. This specialization helps to attain the knowledge required to drive key business decisions. It will also help students develop the necessary skills to carry out analytical procedures and support an organization by figuring out ways to improve and optimize existing business processes with ease.

The cost of the programmes and provision for scholarship have been designed with objective of spreading mass education to meet needs of all class of learners. Personal Contact Programme (PCP) is offered by competent faculty as students' support services which ensures timely response to student's queries and, enhances overall quality standards.

3. NATURE OF PROSPECTIVE TARGET GROUP OF LEARNERS

The Diploma in Cyber Security is designed for a diverse group of learners who are interested in building a strong foundation in information security. This includes higher secondary graduates from any stream (Science, Commerce, or Arts) who are looking to enter the IT or cyber security field. It also targets students from technical or vocational backgrounds such as ITI or polytechnic institutes who wish to enhance their skills. Undergraduates and graduates in computer science, information technology, or related disciplines are also ideal candidates, especially those seeking to specialize in cyber security.

The programme is equally suitable for working professionals in IT roles such as system administrators, network engineers, or technical support staff aiming to upskill and advance in the cyber security domain. Career switchers from non-technical fields who have a keen interest in digital security are also part of the target group. Additionally, small business owners and entrepreneurs who handle digital assets and need to protect their data are encouraged to enroll. The course also benefits individuals preparing for careers in government, defense, or law enforcement where cyber security knowledge is critical. Lifelong learners, educators, and freelance IT consultants interested in expanding their expertise in cyber security also form an important part of the prospective learner group.



4. APPROPRIATENESS OF PROGRAMME TO BE CONDUCTED IN OPEN AND DISTANCE LEARNING (ODL), AND ONLINE MODE TO ACQUIRE SPECIFIC SKILLS AND COMPETENCE

The Diploma in Cyber Security is highly appropriate for delivery through Open and Distance Learning (ODL) and online modes, given the digital nature of the subject and the flexibility it offers to diverse learners. Cyber security education primarily involves theoretical concepts, virtual simulations, and hands-on practice using software tools and online platforms, all of which can be effectively taught and demonstrated through digital learning environments.

ODL and online modes allow learners to access high-quality study materials, video lectures, interactive labs, and virtual environments at their convenience, enabling self-paced learning and flexibility in balancing other responsibilities such as work or education. These modes are particularly suitable for working professionals, remote learners, and those who cannot attend regular on-campus classes due to geographical or financial constraints.

Through online labs, virtual machines, and cloud-based tools, learners can gain practical experience in areas like ethical hacking, network security, malware analysis, and digital forensics. Regular online assessments, peer interactions, discussion forums, and mentorship support further enhance engagement and understanding.

Thus, the programme delivered through ODL and online modes can successfully build the required skills and competencies in cyber security while making education accessible, inclusive, and adaptable to modern learning needs.

All the courses in the programme are theoretical and problem based. So, no laboratory or experiment is needed to impart the skills and competence required for the programme. The specific skill and competencies required for a post graduate can be imparted to a great extent through SLM reference books, E-content and E-tutorial prepared with the approach of self-explanatory self-contained, self-directed, self-motivating and self-evaluating. Centre for Distance and Online Education Department is more costs effective and can take place while continuing full-time employment. The Department offers outcome-based education, having industry centric curriculum. This enables the students to satisfy their needs and aspirations as the system provides enhanced learning opportunities.

4.1 LEARNING OUTCOMES:

Upon successful completion of the Diploma in Cyber Security programme, learners will be able to:

- **Understand Core Concepts:** Demonstrate a thorough understanding of the principles, terminologies, and fundamentals of cyber security.
- **Identify and Analyze Threats:** Identify various types of cyber threats, vulnerabilities, and attack vectors, and analyze their potential impact on systems and networks.
- **Apply Security Measures:** Implement appropriate security controls such as firewalls, antivirus tools, intrusion detection systems, and encryption techniques to protect digital assets.
- **Perform Ethical Hacking:** Conduct ethical hacking and penetration testing in a lawful and professional manner to uncover and address system vulnerabilities.
- **Handle Security Incidents:** Respond effectively to security breaches and incidents by applying knowledge of digital forensics and incident response procedures.
- **Understand Legal and Ethical Aspects:** Exhibit awareness of cyber laws, data protection regulations, and ethical issues related to information security.
- **Use Security Tools Proficiently:** Utilize industry-standard cyber security tools and software for securing networks, systems, and applications.
- **Demonstrate Problem-Solving Skills:** Analyze real-world security challenges and develop logical, practical solutions using critical thinking and technical knowledge.
- **Communicate Effectively:** Prepare clear and concise security reports, and communicate technical information effectively to various stakeholders.
- **Pursue Advanced Learning and Careers:** Be prepared for higher studies in cyber security or take up entry-level roles such as security analyst, network security technician, or IT support in various organizations.

5. INSTRUCTIONAL DESIGN

Need based courses have been identified and the courses are developed. They have been fine-tuned taking into consideration industry/social requirements and also to educate rural people professionally. The course, curriculum and syllabi are designed and evaluated by a Departmental Committee. The curriculum and syllabi are then placed in the Board of Studies. The finalized curriculum and syllabi are then placed in the Academic Council for the final approval. In addition, courses have been introduced specifically for CDOE programmes to suit the requirements of the dynamic changes taking place in the economy and Industry. However, courses can be introduced as and when the need arises after obtaining necessary approvals from the appropriate academic bodies of the University. Approval of Board of

Studies and Academic Council are obtained whenever modifications/additions are made in the existing curriculum and syllabi.

5.1 CURRICULUM DESIGN

The Diploma in Cyber Security is a one-year programme divided into two semesters. The course structure, viz, the scheme and syllabus of the Diploma in Cyber Security is given as under:

Scheme of Diploma in Cyber Security 2025-26

SEMESTER I

Sr. No	Paper Code	Nomenclature of the Paper	Credits	Internal Marks	External Marks	Max. Marks
1.	DCS-11-T	Data Structures	3	30	70	100
2.	DCS-12-T	Data Communication & Networking	3	30	70	100
3.	DCS-13-T	Python Programming	3	30	70	100
4.	DCS-14-T	Cryptography and Network Security	3	30	70	100
5.	DCS-15-T	Operating Systems	3	30	70	100
6.	DCS-16-P	Data Structures Lab.	2	30	70	100
7.	DCS-17-P	Data Communication & Networking Lab.	2	30	70	100
8.	DCS-18-P	Python Programming Lab.	2	30	70	100
Total			21	240	560	800

SEMESTER II

Sr. No	Paper Code	Nomenclature of the Paper	Credits	Internal Marks	External Marks	Max. Marks
1.	DCS-21-T	Ethical Hacking	3	30	70	100
2.	DCS-22-T	Cyber Security	3	30	70	100
3.	DCS-23-T	Internet and Web Technology	3	30	70	100
4.	DCS-24-T	Artificial Intelligence	3	30	70	100
5.	DCS-25-T	Cloud Computing	3	30	70	100
6.	DCS-26-P	Ethical Hacking Lab.	2	30	70	100
7.	DCS-27-P	Cyber Security Lab.	2	30	70	100
8.	DCS-28-MP	Major Project	8	30	70	100
Total			27	240	560	800

Note: To be eligible for the award of the Diploma in Cyber Security, a student has to complete all the 16 courses as shown in the above tables. However, a candidate can take exit option after 6 months (Semester I) and upon successful completion he/she will get Certificate in Cyber Security.

SEMESTER - I

Data Structures

General Course Information

Course Code: DCS-11-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

Unit I

Algorithms and Flowcharts, Basics Analysis on Algorithm, Complexity of Algorithm, Introduction and Definition of Data Structure, Various types of Data Structure, Static and Dynamic Memory Allocation, Arrays, One Dimensional Array and Multidimensional Arrays, Representation and Operation on array, Linked Lists, Representation and Operations of Linked Lists, Singly Linked List, Doubly Linked List, Circular Linked List, Circular Doubly Linked List.

Unit II

Introduction to Stack, Definition, Stack Implementation, Operations of Stack, Applications of Stack: Infix to postfix Transformation, Evaluating Arithmetic Expressions, Introduction to Queue, Definition, Queue Implementation, Operations of Queue, Circular Queue, De-queue and Priority Queue.

Unit III

Introduction to Tree, Tree Terminology Binary Tree, Binary Search Tree, Strictly Binary Tree, Complete Binary Tree, Tree Traversal (pre, post & in-order traversals), Threaded Binary Tree, AVL Tree. Introduction to Graph, Representation to Graphs, Graph traversals (DFS, BFS), Dijkstra Single-Source Shortest Path Algorithm.

Unit IV

Linear and Binary search algorithms, Sorting algorithms: Bubble sort, Selection sort, Insertion sort, Quick sort, Merge sort, Hash Function, Types of Hash Functions, Collision, Collision Resolution Techniques

Text and Reference Books:

1. Seymour Lipschultz, "Data Structures with C (Schaum's Outline Series)", McGraw Hill Education.
2. A. Tanenbaum, Y. Lanhgsamand A. J. Augenstein, "Data Structures Using C", PHI.
3. Seymour Lipschultz, "Theory and Practice of Data Structures", Tata McGraw-Hill.
4. G. S. Baluja, Data Structures through C, 4th Edition – Dhanpat Rai & Co.



Data Communication & Networking

General Course Information

Course Code: DCS-12-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

Unit I

Introduction: Introduction to data communications and networking, use of Computer Networks, classification of networks, OSI model, function of the layers, TCP/IP Protocol suite, Network Topologies: Bus, star, ring, mesh, tree, hybrid topologies with their features, advantages and disadvantages of each type, Transmission Modes: simplex, half duplex and full duplex

Unit II

Transmission Media: Guided Media (Wired) (Twisted pair, Coaxial Cable, Fiber Optics. Unguided Media (Radio Waves, Infrared, Micro-wave, Satellite), Data Communication and Switching Techniques: Framing, flow control, error control, circuit switching, message switching, packet switching

Unit III

Internet addressing system: IP address with their classification and notation, Internet Control Protocols (ARP, RARP, ICMP, IGMP), Routing Protocols (Distant Vector, Link-State)
Switching Devices: Repeaters, hubs, switches, bridges, routers, gateways. Multiplexing: (FDM, WDM, TDM),

Unit IV

Transport layer protocols: TCP and UDP, Internet: Internet, Internet Service Providers (ISPs), Hosts and Domain Names, DNS, WWW, HTTP, URL, FTP, Services: www, Extranet, Email, Applications of Internet

Text and Reference Books:

1. Behrouz A Forouzan, Data Communications and Networking, 5th edition, McGraw Hill, Indian Reprint 2017
2. Douglas E. Comer, Computer Networks and Internet, 6th edition, Pearson Publication, 2015.
3. Andrew S. Tannenbaum, David J. Wetherall, Computer Networks, Pearson Publication, 5th edition.



Python Programming

General Course Information

Course Code: DDS-13-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

Unit I

Introduction to Python, History of Python, Features of Python, Python Identifiers, Python Character Set, Keywords and Indentation, Comments, Command Line Arguments, Assignment Operator, Operators and Expressions, print() Function, input() Function, eval() Function, Python Data Types: int, float, complex, Variables, Mutable vs Immutable variables, Namespaces, Decision Statements: Boolean Type, Boolean Operators, if statement, else statement, Nested Conditionals Statements, Multi-way Decision Statements (elif statement).

Unit II

Loop Control Statements: While loop, range() Function, For Loop, Nested Loops, Infinite Loop, Break Statement, Continue Statement, Pass Statement, Introduction to Strings, String Operations: Indexing and Slicing, Lists: Operations on List: Slicing, Inbuilt Functions for Lists, List Processing: Searching and Sorting, Dictionaries: Need of Dictionary, Operations on Directories: Creation, Addition, Retrieving Values, Deletion; Tuples, operations on Tuples, Inbuilt Functions for Tuples, Introduction to Sets, operations on sets.

Unit III

Python Functions, Inbuilt functions, Main function, User Defined functions, Defining and Calling Function, Parameter Passing, Actual and Formal Parameters, Default Parameters, Global and Local Variables, Recursion, Passing Functions as Data, Lambda Function, Modules, Importing Own Module, Packages. Operations on File: Reading text files, read functions, read(), readline() and readlines(), writing Text Files, write functions, write() and writelines(), Manipulating file pointer using seek, Appending to Files.

Unit IV

Python Object Oriented: Overview of OOP, Classes and objects, Accessing attributes, Built-In Class Attributes, Methods, Class and Instance Variables, Destroying Objects, Polymorphism, Overlapping and Overloading of Operators, Class Inheritance: super(), Method Overriding, Exception Handling, Try-except-else clause, Python Standard Exceptions, User-Defined Exceptions

Text and Reference Books:

1. Martin C. Brown, "Python: The Complete Reference" McGraw Hill Education, Fourth edition, 2018



2. R. Nageswara Rao , “Core Python Programming” Dreamtech Press India Pvt Ltd 2018.
3. Ashok Namdev Kamthane, Programming and Problem Solving with Python, Mc Graw Hill Education Publication, 2018.
4. John Guttag, Introduction to Computation and Programming using Python, Springer
5. Lutz, M., Learning Python: Powerful Object-Oriented Programming. O'Reilly Media, Inc., 2013.
5. Michael T Goodrich and Robertto. Thamassia, Micheal S Goldwasser, Data Structures and Algorithms in Python, Wiley, 2016.
6. Y. Daniel Liang, Introduction to Programming Using Python, Pearson, 2013.
7. Reema Thareja, Python Programming Using Problem Solving Approach , Oxford Publications, 2017.
8. Kenneth A. Lambert, The Fundamentals of Python: First Programs, Cengage Learning, 2011.



Cryptography and Network Security

General Course Information

Course Code: DCS-14-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

Unit I

Cryptography Concept: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, Symmetric key Ciphers: Block Cipher principles, Modes of Operations of Block Ciphers, DES, AES, Stream ciphers

Unit II

Cryptographic Hash Functions: MAC, HMAC, Hash Functions, Cryptographic Hash Functions, Applications of Hash Functions
Asymmetric key Ciphers: Diffie-Hellman Key Exchange Algorithm, RSA, Digital Signatures, Digital Signature Standard.

Unit III

Authentication Application: Kerberos, X.509 Authentication Service, Public Key Infrastructure, Email Security: Pretty Good Privacy (PGP) and S/MIME.
Web Security: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS)

Unit IV

IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Roles of Firewalls - Types of Firewalls - Firewall designs, Intrusion Detection and Prevention Systems

Text and Reference Books:

1. Atul Kahate , Cryptography and Network Security, 2nd edition, Tata Mc Grawhill, India, 2008.
2. BehrouzA.Foruzan," Cryptography and Network Security", Tata McGraw Hill, 2007.
3. Charlie Kaufman, Radia Perlman, and Mike Speciner," Network Security: PRIVATE Communication in a PUBLIC World", Prentice Hall, ISBN 0-13-046019-2.
4. Douglas Stinson, "Cryptography Theory and Practice", Chapman & Hall/CRC, 2nd Edition.

Operating Systems

General Course Information

Course Code: DCS-15-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

Unit I

Need of Operating System, Evolution of Operating System, Types of Operating Systems: Batch, Multi-programming, Time Sharing, Real-Time, Multitasking, Multithreading, Operating System Services, Case Study: Linux, Windows 11

Unit II

Process Model Overview, Programmer's View of Process, Process States, Process and Processor Scheduling: Scheduling Criteria, First Come First Serve, Round Robin, Shortest Job First (SJF), Shortest Remaining Time Next (SRTN), Schedulers, Inter-process Communication and Synchronization: Race Condition, Mutual Exclusion, Monitors, Deadlock: Prevention, Avoidance, Detection and Recovery

Unit III

Overview of Memory Management, Contiguous Allocation: Partitioned Memory Allocation, Fixed & Variable Partitioning, Swapping, Relocation, Protection and Sharing, Non-Contiguous Allocation: Page Allocation, Segmentation, Virtual Memory

Unit IV

Overview of Linux, Installation and Upgrade, Introduction to Shell and Commands: Basic Commands: pwd, cd, mkdir, rmdir, ls, cat, cp, rm, mv, wc, split, cmp, comm, diff, head, tail, grep, sort, apt-get install, apt-get remove, Editing Files with vi, vim, gedit, gcc, Linux Shell Basic Scripts

Text and Reference Books:

1. A. Silberschatz and P. B. Galvin, Operating System Concepts, 8th ed., New Delhi, India: Wiley India,
2. D. M. Dhamdhere, Operating Systems, New Delhi, India: McGraw-Hill Education, Latest Edition.
3. S. Das, UNIX: Concepts and Applications, New Delhi, India: McGraw-Hill Education, Latest Edition.
4. A. K. Harnal, Linux: Application and Administration, New Delhi, India: Tata McGraw-Hill Education, 2009.

Data Structures Lab.

General Course Information

Course Code: DCS-16-P	Course Assessment Methods:
Course Credits: 2	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)

List of Experiments

1. Perform Linear Search and Binary Search on an array.
 - a. Read an array of type integer.
 - b. Input element from user for searching.
 - c. Search the element by passing the array to a function and then returning the position of the element from the function else return -1 if the element is not found.
 - d. Display the position where the element has been found.
2. Implement sparse matrix using array. Description of program:
 - a. Read a 2D array from the user.
 - b. Store it in the sparse matrix form, use array of structures.
 - c. Print the final array.
3. Create a linked list with nodes having information about a student and perform
 - a. Insert a new node at specified position.
 - b. Delete of a node with the roll number of student specified.
 - c. Reversal of that linked list.
4. Create doubly linked list with nodes having information about an employee and perform Insertion at front of doubly linked list and perform deletion at end of that doubly linked list.
5. Create circular linked list having information about an college and perform Insertion at front perform Deletion at end.
6. Create a stack and perform Pop, Push, Traverse operations on the stack using Linear Linked list.
7. Create a Linear Queue using Linked List and implement different operations such as Insert, Delete, and Display the queue elements.
8. Create a Binary Tree (Display using Graphics) perform Tree traversals (Preorder, Postorder, Inorder) using the concept of recursion.
9. Implement insertion, deletion and display (inorder, preorder and postorder) on binary search tree.
10. To implement Quick sort, and Bubble sort using array as a data structure.



Data Communication & Networking Lab.

General Course Information

Course Code: DCS-17-P	Course Assessment Methods:
Course Credits: 2	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)

List of Experiments

(Using Cisco Packet Tracer)

1. **Basic LAN Setup and IP Addressing**
 - a. Create a simple LAN with PCs and switches
 - b. Assign IP addresses and test connectivity with ping
2. **Configuring Switches and VLANs**
 - a. Create VLANs on a switch
 - b. Assign ports to VLANs and verify segmentation
3. **Inter-VLAN Routing**
 - a. Configure router-on-a-stick for communication between VLANs
4. **Static Routing Configuration**
 - a. Configure static routes on routers for inter-network communication
5. **Dynamic Routing Protocol (RIP/OSPF)**
 - a. Implement and verify dynamic routing using RIP or OSPF
6. **Access Control Lists (ACLs)**
 - a. Create and apply standard and extended ACLs to filter network traffic
7. **DHCP Server Configuration**
 - a. Setup DHCP server on router and configure clients for dynamic IP addressing
8. **Network Address Translation (NAT)**
 - a. Configure static and dynamic NAT and PAT for private to public IP translation
9. **WAN Link Simulation**
 - a. Configure serial interfaces and PPP encapsulation with authentication (PAP/CHAP)
10. **Wireless Network Setup**
 - a. Configure wireless router, SSID, and security (WPA2), connect wireless clients
11. **Spanning Tree Protocol (STP) Configuration**
 - a. Enable STP on switches to prevent network loops and verify operation
12. **Basic Network Troubleshooting**
 - a. Use Cisco IOS commands (ping, tracert, show ip route, etc.) to diagnose and resolve network issues

Python Programming Lab.

General Course Information

Course Code: DCS-18-P	Course Assessment Methods:
Course Credits: 2	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)

List of Experiments

1. Install Python and explore various popular IDE like IDLE, PyCharm, and Anaconda.
2. Assignments to perform various number operations like
 - a. Find maximum from a list of numbers
 - b. GCD of two number
 - c. Square root of a number
 - d. Check number is prime or not.
 - e. Print first N prime numbers
 - f. Remove duplicate numbers from list
 - g. Print the Fibonacci series.
3. Assignments to perform various operations on Strings like creation, deletion, concatenation.
4. Create a List L = [10, 20, 30]. Write programs to perform following operations:
 - a. Insert new numbers to list L.
 - b. Delete numbers from list L.
 - c. Sum all numbers in list L.
 - d. Sum all prime numbers in list L.
 - e. Delete the list L.
5. Create a Dictionary D= {'Name': 'Allen', 'Age': 27, 5:123456}. Write programs to perform following operations:
 - a. Insert new entry in D.
 - b. Delete an entry from D.
 - c. Check whether a key present in D.
 - d. Update the value of a key.
 - e. Clear dictionary D.
6. Two assignments on Sets to perform various operation like union, intersection, difference etc.
7. Two assignments related to searching operation like linear search, binary search.
8. Three assignments related to sorting like selection sort, bubble sort, insertion sort.
9. Demonstrate the use of dictionary for measuring student marks in five subjects and you have to find the student having maximum and minimum average marks.
10. Two assignment on usage of different available packages like random package to perform
 - a. Print N random numbers ranging from 100 to 500.
 - b. Print 10 random strings whose length between 3 and 5.
11. Implement and demonstrate the functions of a simple calculator.
12. One assignment on implementing object oriented concept such as classes, inheritance, and polymorphism.

SEMESTER - II

Ethical Hacking

General Course Information

Course Code: DCS-21-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

UNIT I

Introduction to Ethical Hacking, Who is a Hacker?, What is Ethical Hacking?, Types of Hackers: White Hat, Black Hat, Grey Hat, Key Terminologies: Adware, Botnet, Brute Force Attack, Phishing, Malware, Rootkit, SQL Injection, Trojan, Virus, Vulnerability, Worms, Cross-Site Scripting, Security Concepts, Developing an Ethical Hacking Plan

UNIT II

Common Tools: Nmap, Metasploit, Burp Suite, Angry IP Scanner, Cain and Abel, Phases of Ethical Hacking: Reconnaissance (Active & Passive), Scanning, Gaining Access, Maintaining Access, Clearing Tracks, Reporting, Footprinting: Domain Name Info, IP Address, Hosting Company, IP Ranges, Website History, Footprinting Tools

UNIT III

Fingerprinting: Active & Passive, Port Scanning, Ping Sweep, DNS Enumeration, Enumeration Basics: NTP Suite, enum4linux, Sniffing: Purpose, Techniques, Tools, ARP Poisoning, MITM Attack, DNS Poisoning (Concept & Prevention), Trojan Attacks: Detection & Prevention, TCP/IP Hijacking, Email Hijacking, Password Hacking: Dictionary Attack, Hybrid Attack, Brute-Force Attack

UNIT IV

Wireless Hacking: Kismet, NetStumbler, WEP Attacks, Social Engineering: Phishing and Prevention, Web Hacking: Cross-Site Scripting (XSS), SQL Injection (sqlmap, sqlninja), Basics of Scripting for Hacking: Python, PHP (Overview only), Penetration Testing: Types, Steps, Essential Tools, Ethical Guidelines

Text and Reference Books:

1. Joe Grant, Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Understand the Concept of Ethical Hacking, Independently Published, 2023.

2. Jon Erickson, Hacking: The Art of Exploitation, 2nd Edition, No Starch Press, 2008.
3. Patrick Engebretson, The Basics of Hacking and Penetration Testing, 2nd Edition, Syngress, 2013.
4. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley, 2011.
5. Michael Gregg, Certified Ethical Hacker, 3rd Edition, Pearson IT Certification, 2019.
6. Roger A. Grimes, Hacking the Hacker, 1st Edition, Wiley, 2017.
7. Ankit Fadia, The Unofficial Guide to Ethical Hacking, 2nd Edition, Laxmi Publications, 2006.
8. Randy Weaver, Dawn Weaver, and Dean Farwood, Guide to Network Defense and Countermeasures, 3rd Edition, Cengage Learning, 2014.



Cyber Security

General Course Information

Course Code: DCS-22-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Course Content

Unit I

Introduction to Cyber Security, Importance and challenges in Cyber Security, Cyberspace, Cyber threats, Cyber warfare, CIA Triad (Confidentiality, Integrity, Availability), Cyber Terrorism, Security of Critical Infrastructure, Hacking, Cracking, Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Viruses, Worms, Trojans, Logic Bombs, Time Bombs, Email Bombing, Data Diddling, Salami Attacks, Phishing, Steganography, Cyber Stalking, Spoofing, Defamation, Computer Vandalism, Crimes in Social Media, Adware, Scareware, Ransomware, Social Engineering, Credit Card Frauds, Financial Frauds, Telecom Frauds,

Unit II

Computer Counterfeiting, Software Piracy, Spamming, Man-in-the-Middle Attack, Drive-by Attack, Password Attack, SQL Injection Attack, Cross-site Scripting Attack, Eavesdropping Attack, Birthday Attack, Hackers and Crackers, Cyber Attacks and Vulnerabilities, Malware threats, Sniffing, Gaining Access, Hiding Files, Covering Tracks, Backdoors, Vulnerabilities in Software, Vulnerabilities in System Administration, Threat Actors, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband Communications,

Unit III

Access Control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Endpoint Device Security, Mobile Phone Security, Password Policy, Security Patch Management, Data Backup, Management of Third-party Software, Device Security Policy, Cyber Security Best Practices, Host Firewall, Anti-virus, Management of Host Firewall, Management of Anti-virus, Wi-Fi Security, Configuration of Security Policies and Permissions.

Unit IV

Evolution of the IT Act, IT Act 2000, Amendments to the IT Act, Authorities under the IT Act and their Powers, Penalties under the IT Act, Offences under the IT Act, Recent Amendments, National and International Cyber Laws Overview, Intellectual Property Rights, Domain Names, Trademark Disputes, Copyright in Computer Programmes, Patent Rights, Cyber Ethics, Principles of Cyber Ethics, Code of Conduct in Cyberspace, Social Aspects of Cyber Ethics, Legal Aspects of Cyber Ethics.

Text and Reference Books:

1. Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 4th Edition, Cengage Learning, 2011.

2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Education, 2017.
3. Atul Kahate, Cryptography and Network Security, 4th Edition, McGraw Hill Education, 2019.
4. Nina Godbole and Sumit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, 1st Edition, Wiley India Pvt. Ltd., 2011.
5. R. C. Mishra, Cyber Crime Impact in the New Millennium, Author Press, 2010.
6. Henry A. Oliver, Security in the Digital Age: Social Media Security Threats and Vulnerabilities, CreateSpace Independent Publishing Platform, 2013.
7. Elias M. Awad, Electronic Commerce, Prentice Hall of India Pvt. Ltd., 2002.
8. Kumar K, Cyber Laws: Intellectual Property & E-Commerce Security, Dominant Publishers, 2005.
9. Eric Cole, Ronald Krutz, and James W. Conley, Network Security Bible, 2nd Edition, Wiley India Pvt. Ltd., 2009.
10. E. Maiwald, Fundamentals of Network Security, McGraw Hill Education, 2003.



Internet and Web Technology

General Course Information

<p>Course Code: DCS-23-T Course Credits: 3</p> <p>Exam Duration: 3 hours</p>	<p>Course Assessment Methods:</p> <p>Max. Marks: 100</p> <p>(Internal Marks: 30; External: 70)</p> <p>Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.</p>
--	---

Course Content

Unit I

Basics of WWW, HTTP protocol, Client-Server architecture, Introduction to web server: installation and configuration, Internet, URL (Uniform Resource Locator), Internet Service Provider, Intranet, Extranet, Virtual Private Network

Web Design fundamentals: Concepts of effective web design, Web design issues, Page Layout and linking, User-centric design, Sitemap, Planning and publishing website, Designing effective navigation

Unit II

Basics of HTML: Introduction to HTML, Create a Web page, Linking to other Web Pages, Publishing HTML Pages, Text Alignment and Lists, Text Formatting Fonts Control, Email Links and link within a Page, Creating a Table, Creating HTML Forms, Creating Web Page Graphics, Putting Graphics on a Web Page, Custom Backgrounds and Colors, Creating Animated Graphics

Unit III

Cascading Style Sheet: Need for CSS, introduction to CSS, basic syntax and structure, using CSS, background images, colors and properties, manipulating texts, using fonts, borders and boxes, margins, padding lists, positioning using CSS, XML: Introduction of XML- Some current applications of XML, Features of XML, Anatomy of XML document, The XML Declaration, Element Tags- Nesting and structure, XML text and text formatting element

Unit IV

Introduction to JavaScript , Variable Naming Rules and JavaScript Data Types, Expressions and Operators, Flow Control, Objects and Arrays, Defining Functions and Methods , The Document Object Model (DOM), How to Get Input and Output, JavaScript in Browsers, Handling Web Page Events



Text and Reference Books:

1. Bhaumik Shroff, *Introduction to Internet & HTML Scripting*, 3rd Edition, Books India Publication, 2005.
2. Raj Kamal, Satinder Bal Gupta, and Brij Mohan Goel, *Internet and Web Technologies*, Tata McGraw-Hill, 2012.
3. Dick Oliver, *Teach Yourself HTML 4 in 24 Hours*, 4th Edition, TechMedia, 2000.
4. Thomas Powell and Fritz Schneider, *JavaScript: The Complete Reference*, 2nd Edition, McGraw Hill Education, 2004.
5. Thomas A. Powell, *HTML: The Complete Reference*, Tata McGraw Hill, 2003.
6. Kynn Bartlett, *CSS: The Complete Reference*, 2nd Edition, Pearson Education, 2002.
7. Dick Oliver and Michael Morrison, *HTML and CSS: Visual QuickStart Guide*, 7th Edition, Pearson Education, 2010.
8. Kogent Learning Solutions Inc., *Web Technologies: HTML, JavaScript, PHP, Java, JSP, ASP.NET, XML and Ajax*, Wiley India Ltd., 2009.
9. Michael Young, *XML Step by Step*, 2nd Edition, PHI Learning, 2002.
10. G. P. Moseley and P. S. Savaliya, *Web Technology*, Wiley India, 2010.



Artificial Intelligence

General Course Information

<p>Course Code: DCS-24-T Course Credits: 3 Exam Duration: 3 hours</p>	<p>Course Assessment Methods: Max. Marks: 100 (Internal Marks: 30; External: 70)</p> <p>Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.</p>
---	---

Course Content

Unit I

Overview of Artificial Intelligence: Introduction to AI, Importance of AI, AI and its related field, Turing Test, Intelligent Agents – Agents and Environments – Good Behavior – Nature of Environments – Structure of Agents, Problem Solving Agents.

Unit II

Searching for solutions, Uninformed Search Strategies – Informed Search Strategies, Heuristic functions - Adversarial search - Local search algorithms and optimization problems – Searching with nondeterministic actions, Constraint satisfaction problems.

Unit III

Knowledge and reasoning Logical Agents: Wumpus world - Propositional logic - First order logic: Inference, forward and backward chaining, Resolution, Planning Classical planning – Algorithms – Approaches - Planning and acting in real world – Hierarchical planning – Multiagent planning.

Unit IV

Introduction to Machine learning terminologies – Types of Machine learning, Data Preprocessing – Real world applications: Classification – Regression – Clustering , Ensemble Learning, Introduction to Neural Network and Deep learning

Text and Reference Books:

1. Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th Edition, PHI Learning, 2022.
2. Dan W. Patterson, *Introduction to Artificial Intelligence and Expert Systems*, 1st Edition, PHI Learning, 1995.
3. Aurélien Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, O'Reilly, 2019.
4. Sebastian Raschka, Yuxi (Hayden) Liu, and Vahid Mirjalili, *Machine Learning with PyTorch and Scikit-Learn: Develop Machine Learning and Deep Learning Models with Scikit-Learn and PyTorch*, Packt Publishing, 2022.



5. Elaine Rich, Kevin Knight, and Shivashankar B. Nair, *Artificial Intelligence*, McGraw Hill Education, 2009.
6. Rajiv Chopra, *Artificial Intelligence: A Practical Approach*, S. Chand Publishing, 2012.
7. Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, Pearson Education, 3rd Edition, 2015.
8. Dan W. Patterson, *Introduction to Artificial Intelligence and Expert Systems*, 1st Edition, Pearson Education, 2007.
9. Deepak Khemani, *A First Course in Artificial Intelligence*, McGraw Hill Education, 2013.
10. George F. Luger, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*, 5th Edition, Pearson Education, 2009.
11. Gavin Hackeling, *Mastering Machine Learning with Scikit-Learn: Learn to Implement Machine Learning Algorithms Effectively*, Packt Publishing, 2017.



Cloud Computing

General Course Information

Course Code: DCS-25-T	Course Assessment Methods:
Course Credits: 3	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)
	Examiner will be required to set nine questions in all. First question will be compulsory, consisting of objective type/short answer type questions covering the entire syllabus. In addition to that eight more questions will be set, two questions from each unit. A candidate will be required to answer five questions in all, selecting one question from each unit in addition to compulsory question number one. All questions will carry equal marks.

Unit I

Overview of Cloud Computing- Cloud at a Glance: The Vision of Cloud Computing, Defining a Cloud, Cloud Computing Reference Model, Characteristics and Benefits, Historical Developments: Distributed Systems, Cluster Computing, Grid Computing, Virtualization.

Unit II

Virtualization & Cloud Computing Architecture – Introduction, Characteristics of Virtualized Environments, Taxonomy of Virtualization Techniques: Execution Virtualization, Other Types of Virtualization, Virtualization and Cloud Computing: Pros and Cons of Virtualization, Cloud Architecture: Introduction, Cloud Reference Model Architecture, Infrastructure as a Service, Platform as a Service, Software as a Service, Types of Clouds: Public, Private, Hybrid, Community,

Unit III

Cloud in Industry and Its Applications – Amazon Web Services: Compute Services, Storage Services, Communication Services, Additional Services, Google AppEngine: Architecture and Core Concepts, Application Life-Cycle, Microsoft Azure: Core Concepts, SQL Azure, Windows Azure Platform Appliance, Cloud Applications in various domains.

Unit IV

Security in Cloud – Cloud Information Security Fundamentals, Cloud Security Services, Design Principles, Secure Cloud Software Requirements, Policy Implementation, Cloud Computing Security Challenges, Virtualization Security Management, Cloud Computing Security Architecture.

Text and Reference Books:

1. Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi, *Mastering Cloud Computing*, McGraw Hill Publication (India) Private Limited, 2013.
2. Krutz, Vines, *Cloud Security*, Wiley Publication, 2010.
3. Bloor R., Kanfman M., Halper F. Judith Hurwitz, *Cloud Computing for Dummies*, (Wiley India Edition), 2010.
4. John Rittinghouse & James Ransome, *Cloud Computing Implementation Management and Strategy*,



CRC Press, 2010.

5. Antohy T Velte , *Cloud Computing : A Practical Approach*, McGraw Hill, 2009.
6. Rajkumar Buyya, James Broberg and Andrez Gossinski, *Cloud Computing: Principles and Paradigm*, John Wiley and Sons, Inc. 2011.
7. Kai Hwang, Geofferyu C. Fox and Jack J.Dongarra, *Distributed and Cloud Computing*, Elsevier, 2012.



Ethical Hacking Lab.

General Course Information

Course Code: DCS-26-P	Course Assessment Methods:
Course Credits: 2	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)

List of Experiments

1. Set up Kali Linux in a virtual machine and set up a network adapter.
2. Scan the network for Kali Linux and Windows target machines in local network and virtual network.
3. Identify the open ports using NMAP.
4. Use password guessing tools to guess a ZIP file password.
5. Extract password hashes from Windows machines.
6. Experiments on Metasploit framework.
7. Website Information Gathering techniques.
8. Experiments on SQL injections.
9. Implement a code to simulate buffer overflow attack.
10. Prevention against cross site scripting attacks.



Cyber Security Lab.

General Course Information

Course Code: DCS-27-P	Course Assessment Methods:
Course Credits: 2	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)

List of Experiments

1. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.
2. Study of packet sniffer tools like Wireshark, ethereal, tcpdump etc. Use the tools to do the following.
3. Observe performance in promiscuous as well as non-promiscuous mode.
4. Show that packets can be traced based on different filters.
5. Download and install NMAP. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, TCP port scan, UDP port scan, etc.
6. Detect ARP spoofing using open source tool ARPWATCH.
7. Use the Nessus tool to scan the network for vulnerabilities.
8. Set up IPSEC under LINUX.
9. Install IDS (e.g., SNORT) and study the logs.
10. Use of iptables in Linux to create firewalls.



Major Project

General Course Information

Course Code: DCS-28-MP	Course Assessment Methods:
Course Credits: 8	Max. Marks: 100
Exam Duration: 3 hours	(Internal Marks: 30; External: 70)

Students are required to complete their project work in the domain of Cyber Security by the end of 2nd semester. Students carry out implementation of their respective projects based on the problem identified, methodology and tools suggested in the synopsis submitted in the second week in the starting of 2nd semester. They prepare the final project reports according to the format provided. At the end of 2nd semester, each student is required to present his/her project work in front of internal project guide and external examiner appointed by Controller of Examination.



5.2 DURATION OF PROGRAMME

The duration of the Diploma in Cyber Security is one year and the maximum duration is three years.

1. A student who for whatever reasons is not able to complete the programme within the normal period or the minimum duration prescribed for the programme shall be allowed two years period beyond the normal period to clear the backlog to be qualified for the degree. The general formula, therefore, will be as follows:
 - a) Time span = $N+2$ years for the completion of programme. Where N stands for the normal or minimum duration prescribed for completion of the programme.
 - b) In exceptional circumstances a further extension of one more year may be granted. The exceptional circumstances are spelt out clearly by the relevant statutory body of the University.
2. Further, the mercy chance, if any will be given within maximum allowed period of the programme as per UGC guidelines. In normal circumstances, only two chances will be given to pass re -appear examination.

5.3 FACULTY AND SUPPORT STAFF

FACULTY

The Centre for Distance & Online Education (CDOE) have qualified teaching faculty to look after the programme as a programme coordinator. They look for the following activities related to the distance education:

- Conducting Personal Contact Programme (PCP) classes for the students.
- Assisting in the change of Regulations and Curriculum, admission work, counseling new students and other issues such as break of study, exemptions etc.
- Coordinating for the preparation of study materials for all semesters/year.
- Coordinating with the faculty members for the preparation and evaluation of assignments of students, and viva voce examinations.

SUPPORT STAFF

The Centre for Distance and Online Education (CDOE) of the university is headed by the director who is a full-time faculty member (Professor) of the university appointed by Vice-Chancellor to facilitate the development, implementation and monitoring the programmes offered at CDOE and to attend all administrative matters concerned with the activities of

directorate. The supporting staffs such as one Deputy Registrar, one Assistant Director, one Superintendent, two Deputy Superintendent, one Hindi Officer, Six Assistants and other clerical staff are coordinating the activities of Centre for Distance and Online Education (CDOE) and looks after the problems of the students. The Supporting staff looks after the problems of the students through online admission help line, examination related work, study material delivery, grievance redressal and so on. The CDOE is assisted by the IT CELL for the online uploading and evaluation of assignments and other student support activities. The CDOE also assisted by Pt. Deendayal Upadhyaya Computer and Informatics Centre (PDUCIC) department for communicating important information to the students through CDOE website of Guru Jambheshwar University of Science and Technology, Hisar. The PDUCIC department managed the CDOE Website of the University. There are six faculties of commerce & management in the Centre for Distance and Online Education who are looking after the programme as programme coordinator(s) and course co-ordinator(s). Further, support from faculties of parent teaching department

5.4 INSTRUCTIONAL DELIVERY MECHANISM

The Instructional delivery mechanisms of the University for ODL/online courses different components, viz, SLM, Personal Contact Programme (PCP), E-Content, E-Tutorial, Internal Assignments and End Term Examination.

- **Self Learning Material**– The success and effectiveness of the department largely depends on the e-content in the form of self-learning mode (SLM). So, it is necessary that the online study material must be ideal for easy and better understanding. Learning Material through electronic media named Self-learning Material (SLM) is developed with the approach of self-explanatory, self-contained, self-motivating and self-evacuating followed by the UGC guidelines.
- **Personal Contact Programme**- PCP sessions guide the learners as the programme proceeds. The PCP schedule is communicated to the learners through our website or Email service. During PCP, the learner gets guidance for better understanding of the programme and subject. The Personal Contact Programme (PCP) is arranged for each of the course by respective Programme Coordinator. The learners get their doubts cleared with the help of subject experts sop as to improve their self-learning capability. Learners are required to attend PCP sessions for all their respective subjects.
- **E-Contents**– The success and effectiveness of online distance education systems largely depends on the e-content in the form of self-learning mode (SLM). So, it is necessary that

the online study material must be ideal for easy and better understanding. Learning Material through electronic media named Self-learning Material (SLM) is developed with the approach of self-explanatory, self-contained, self-motivating and self-evaluating followed by the UGC guidelines. Beside this, the E-content also may include e-book, illustrations, case studies, presentations and web resources such as further references, related links, open-source content on internet, video, case studies, research papers, journals, anecdotal information, articles, historical development of the subject etc.

- **E-Tutorial** – E-Tutorial in the form of video-audio lectures, PPTs, virtual labs etc., guide the learners for better insights on subject matters. It shall be the responsibility of the programme coordinator to ensure that none of the graphics, animation, images, sound clips, video clips used are plagiarized or cited without formal permission from owners. The information for the e-tutorial is communicated to the learners through our website or SMS Services. During e-tutorial, the learner gets guidance for better insights of the subject. A five credit course shall typically have 20 hours of video content and 20 hours of reading material.
- **Discussion Forum:** The facility of discussion forum also provided for raising of doubts and clarifying the same on real time basis for programme by the respective Programme Coordinator and his/her team. The learners get their doubts cleared with the help of subject experts so as to improve their self- learning capability. Learners are required to attend e-tutorial as well as discussion forum sessions for all their respective subjects. The mentor shall be the subject matter expert adept in handling technology. The Programme coordinator and mentor shall need to participate actively in discussion forum. Apart from discussion forum other interactive platforms like web conferencing may also be used.
- **Internal Assessments-** Centre for Distance and Online Education learners have to depend much on self-study. In order to ascertain the writing skill and level of comprehension of the learner, assignment work is compulsory for all learners. The Centre for Distance and Online Education (CDOE) of this university has an online portal for the uploading of the assignments and same has been evaluated online by the subject expert. Two assignments of 30 marks i.e. 15 marks each is allotted for each subject consists of questions with-practical based. The assignment question papers are uploaded on the website within a scheduled time and the learners are required to respond them within a specified period of time. The response of the learner is examined by a faculty member.



- **End Term Examination-** At the end of every session, learners will give theory exam for 70 marks for each subject. For examination (ODL Mode/Online Mode), there will be of nine questions. The first question will be compulsory consisting of seven short questions of two marks each covering the entire syllabus (all four Units). In addition, eight more questions of 14 marks each will be set comprising from the entire syllabus and the students are required to attempt any four questions from these. The online mode examination will be conducted either using computer-based test or pen and paper test in a proctored environment in designated test center with all the security arrangements ensuring transparency and credibility of the examinations. Online examination may also be conducted through technology mediated proctoring.

5.5 STUDENT SUPPORT SERVICES

The department of the university provides the Student Support Services through online mode. Following are the main student support services provided by university through online mode:

- Online Admission Portal for students
- Online fee portal for students
- SMS alert facility for the students for information related to PCPs, Project, Deadlines and Viva-voce etc.
- Grievance handling mechanism is adopted with the help of supporting technical staff
- Practical Questions Based Assignments
- Online availability of Old Question Papers and study material
- Comprehensive viva-voce is conducted after term end examination in the University
- Student Help Desk

6. PROCEDURE FOR ADMISSIONS, CURRICULUM TRANSACTION AND EVALUATION

6.1 PROCEDURE FOR ADMISSIONS

6.1.1 Admission Procedure

Whole admission process is online as per the University rules.

6.1.2 Admission policy for the programme

Admission is based on filling online Admission Form. The procedure of filling the online application form is a four-step procedure, i.e.

- Candidate Registration.

- Payment option through Net Banking, Debit card or Credit card.
- Filling of application form.
- Uploading required scanned documents.
- Generating Preview

6.1.3 Eligibility

Sr. No.	Title of Programme	Eligibility
1.	Diploma in Cyber Security	12 th pass in any discipline

6.1.4 Fee structure

Diploma in Cyber Security (ODL Mode)

Installment No.	Amount	Without late fee	With late fee of ₹ 1000/- per month
1 st Installment	₹ 7,500/-	At the time of admission	-
2 nd Installment	₹ 4,500/-	31 st January every year	30 th April every year

Diploma in Cyber Security (Online Mode)

Installment No.	Amount	Without late fee	With late fee of ₹ 1000/- per month
1 st Installment	₹ 10,500/-	At the time of admission	-
2 nd Installment	₹ 7,500/-	31 st January every year	30 th April every year

6.1.5 Curriculum Transaction

The Centre for Distance and Online Education supply study material in the form of self learning mode (SLM), printed books/lessons as well as in the electronic form. The students get the same directly from the department either by hand or will be sent by post/courier service. Similarly, soft copy of the SLM is uploaded on the CDOE website. Personal contact programme (PCP) for students is also arranged by the expert teachers to resolve the queries and doubt regarding the syllabus. E-tutorial for programme is arranged for each semester by the respective Programme Coordinator. Theory/Practical teaching as per requirements will be provided to the students by the subject specialists. Video lectures are also provided to the students on their LMS portal. The e-tutorial held as per the schedule given in the prospectus. In addition to this student are informed about e-tutorial and other activities through website and mail as well.

6.1.5 Evaluation

Internal assessment will be based on practical assignments and the evaluation will be done by experts in relevant field. External term end evaluation is done by experts in relevant field.

Last Date of online submission of Internal Assignments

Odd Semester	Even Semester
15 th January every year	30 th April every year
Last Date of submission of Internal Assignment with a late fee of Rs. 500/-	
31 st January every year	31 st May every year
Last Date of submission of Internal Assignment with a late fee of Rs.1000/-	
15 th February every year	15 th June every year

NOTE:

1. The students have to upload two internal handwritten assignments of each theory paper of 30% weightage in the stipulated time period mentioned above. Assignments will be prepared by the students will be available on the CDOE website and student portal/LMS as well. It is the sole responsibility of the student to download the question paper of the assignment and upload the solved assignments.
2. The students who fail in internal assessment as well as in aggregate will have the option to improve their score in the internal assessment giving a special chance to such students.
3. A student who could not score 40% marks in external examination of the particular course will have to reappear in the external examination of the respective paper as per university rules in this connection.

7. REQUIREMENT OF THE LABORATORY SUPPORT AND LIBRARY RESOURCES

7.1 Laboratory Support:

A well-equipped Computer lab with latest version of MS Office and internet facility is also available in the department of Centre for Distance and Online Education of this university. This Computer Lab is established with an aim to meet the computing requirements of all the learners of the University. This lab is equipped with 12 desktop computers of latest configuration i.e. Window 7, Window 10 and I3 processor. In addition to this, there is one printer, one scanner and one LED in the Computer Lab for teaching through presentation and video lectures to students. There is one lab attendant for handling the queries regarding online admission, fee payment, uploading of assignments, any other queries through mail, etc.

7.2 Library Resources:

The infrastructure related to library resources is available in the present set-up of the university whereby, we have a well stacked library with latest books, journals, magazines and newspapers. It is named after the great Indian Jurist, Economist, Politician and Social reformer Dr. Bhim Rao Ambedkar. The seating capacity of the University Library is 400 seats. By the end of December 2018, the Library has a collection of 106566 books. The library in its electronic repository has the access to 7000+ e-journals from 14 publishers and 5 Databases. Moreover, 2149 e-books of national and international repute publishers have also been added in e-repository to enrich the students, but within the university premises. University library provides different services to distance learners such as Air-Conditioned Reading Halls, Reading Facility for 400 students, Laptop Lab for SC/ST students consisting of 20 Laptops with internet facility and Potable Water facility on every floor. The online e-library resources namely INFLIBNET is also available for the accessibility of books and journals.

8. COST ESTIMATE OF THE PROGRAMME AND THE PROVISIONS

Cost estimates of programme are based on following components:

- Study Material development and delivery such as cost of writing, vetting, editing, SLM conversion, printing and dispatch etc.
- Personal Contact Programme (PCP) related activities
- E-tutorial/Video Lectures
- Proctored examination and evaluation
- Internal assessment preparation and evaluation
- Miscellaneous cost like advertising on FM radio broadcast, newspapers and SMS alert
- Salary to Teaching and Non-Teaching Staff

9. QUALITY ASSURANCE MECHANISM

9.1 Quality Policy of University:

The Guru Jambheshwar University of Science & Technology (GJUST) is committed to achieve excellence in teaching, research, and extension by follow and implement following points of quality policy:

- Imparting globally competitive education
- Selecting and retaining competent and motivating faculty



- Providing state of the art infrastructural resources
- Promoting quality research culture
- Ensuring transparent and accountable governance
- Focusing on holistic development of learners
- Symbiotic relationship with industry, other academic institutions, and society
- Striving for financial self-reliance

9.2 Advisory Committee:

The Advisory Committee headed by the Vice-Chancellor has been constituted to monitor the activities of the Department along-with matters related to quality assurance (Functions and List of members attached). Following is the composition of Advisory Committee:

1	Vice Chancellor, GJUS&T	Chairperson
2	Registrar, GJUS&T	Member
3	Dean Academic Affairs, GJUS&T	Member
4	Dean of Colleges, GJUS&T	Member
5	Controller of Examination, GJUS&T	Member
6	Prof. Sandeep Rana, (TA-HRM), GJUS&T	Member
7	Chairperson, Department of CSE, GJUS&T	Member
8	Director, HSB, GJUS&T	Member
9	Chairperson, Department of Mass Communication, GJUS&T	Member
10	Director, DE, KUK	Member
11	Prof. R. Baskar, IGNOU, Delhi	Member
12	Director, DE, MDU	Member
13	Director, PDUCIC, GJUS&T	Member
14	Dy. Registrar (CDOE), GJUS&T	Member
15	DR/AR (Accounts), GJUS&T	Member
16	DR/AR (Academic), GJUS&T	Member
17	Director, Centre for Distance and Online Education, GJUS&T	Member Secretary

9.3 Centre for Internal Quality Assurance (CIQA)

The CIQA also oversees the development and preparation of SLMs, then it is submitted to the Board of Studies concerned for the approval. The objective of establishment of Centre for Internal Quality Assurance (CIQA) is to develop and put in place a comprehensive and



dynamic internal quality assurance system to provide high quality programmes of higher education in the Open and Distance Learning mode.

CENTRE FOR INTERNAL QUALITY ASSURANCE (C.I.Q.A.)		
1	Vice Chancellor, GJUS&T	Chairperson
2	Registrar, GJUS&T	Member
3	Dean Academic Affairs, GJUS&T	Member
4	Dean of Colleges, GJUS&T	Member
5	Controller of Examination, GJUS&T	Member
6	Prof. Sandeep Rana, (TA-HRM), GJUS&T	Member
7	Chairperson, Department of CSE, GJUS&T	Member
8	Director, HSB, GJUS&T	Member
9	Chairperson, Department of Mass Communication, GJUS&T	Member
10	Director, DE, KUK	Member
11	Prof. R. Baskar, IGNOU, Delhi	Member
12	Director, DE, MDU	Member
13	Director, PDUCIC, GJUS&T	Member
14	Dy. Registrar (CDOE), GJUS&T	Member
15	DR/AR (Accounts), GJUS&T	Member
16	DR/AR (Academic), GJUS&T	Member
17	Director, Centre for Distance and Online Education, GJUS&T	Member Secretary

9.3 Functions of Centre for Internal Quality Assurance (CIQA)

Following are the main functions of CIQA:

- To maintain quality in the services provided to the learners.
- To ensure continuous improvement in the entire operations of the Higher Education Institution.
- To identify the key areas in which the Higher Education Institution should maintain quality.
- To disseminate information on quality assurance.
- To device mechanisms for interaction and obtaining feedback from various Departments or Centres or Schools in the Higher Education Institution.



- To suggest to the authorities of the Higher Education Institution, measures for qualitative improvement.
- To ensure the implementation of its recommendations through regular monitoring.
- To ensure participation of all stake holders namely, learners, teachers, staff, parents, society, employers and Government in Quality Improvement Process.
- To prepare Programme Project Report and ensure another launch of programme(s).
- Collection, collation and dissemination of accurate, complete and reliable statistics about the quality of the programme(s).

9.4 Activities of Centre for Internal Quality Assurance (CIQA)

Following are the main activities of CIQA:

- Prepare a Programme Project Report (PPR) for each programme according to the norms and guidelines prescribed by the Commission and wherever necessary by the appropriate regulatory authority having control over the programme;
- Get the Programme Project Report (PPR) approved by the appropriate authority of the Higher Educational Institution and the Commission before launch of the programme;
- Oversee the development of Study Learning Material (SLM), e-Content, e-tutorial, integration of Information and Communication Technology (ICT), setting up of Learning Centres and coordination with the parent institution and relevant Regulatory authorities;
- Put in place monitoring mechanism to ensure the proper implementation of Programme Project Reports (PPRs);
- Design annual plans for quality level enhancement at the level of the Higher Educational Institution and ensure their implementation;
- Arrange for feedback responses from students, employers and other stakeholders for quality related institutional processes;
- Develop quality benchmarks or parameters for the various academic and administrative activities of the Higher Educational Institution;
- Obtain information from other Higher Educational Institutions on various quality benchmarks or parameters and best practices;
- Organize workshops or seminars on quality related themes and Higher Educational Institution wise dissemination of the proceedings of such activities;
- Suggest restructuring of programmes in order to make them relevant to the job market;
- Develop and implement innovative practices in major areas leading to quality enhancement in services to the learners;
- Create learner centric environment rather than institution centric environment;



- Adopt measures to ensure internalisation and institutionalisation of quality enhancement practices through periodic accreditation and audit;
- Conduct or encourage system-based research to bring about qualitative change in the entire system;
- Coordinate between the Higher Educational Institution and the Commission for various quality related issues or guidelines;
- Record activities undertaken on quality assurance in the form of an annual report; and
- To coordinate recognition and accreditation of the Higher Educational Institution.

10. PROGRAMME OUTCOMES

The Diploma in Cyber Security programme is designed to produce graduates who possess a balanced blend of theoretical knowledge and practical skills in securing digital information and infrastructure. Upon successful completion of the programme, learners will be able to contribute effectively to the protection of computer systems and networks, understand the legal and ethical aspects of the field, and apply critical thinking to solve real-world security problems. The programme also prepares students for further education or professional roles in the rapidly growing cyber security industry. The programme is aimed at following outcomes:

- **PO1:** Learners will acquire a comprehensive understanding of cyber security concepts, principles, threats, and defense mechanisms.
- **PO2:** Graduates will be able to apply theoretical knowledge to real-world scenarios by using industry-standard tools and techniques.
- **PO3:** Students will develop awareness of cyber laws, data privacy regulations, and ethical standards. They will be able to practice responsible behavior in the cyber world, respecting intellectual property, user privacy, and legal boundaries.
- **PO4:** Learners will enhance their communication skills to effectively report and present security findings. They will also develop the ability to work collaboratively in teams and apply logical reasoning and critical thinking to identify and solve security problems efficiently.
- **PO5:** Graduates will be equipped with the motivation and foundation for continuous learning to keep pace with evolving cyber threats and technologies. They will be ready to pursue higher education, professional certifications, or begin a career in cyber security roles across various industries.

