SKILL ENHANCEMENT COURSES

SYLLABUS FOR THE

SUBJECT: COMPUTER SCIENCE

for the award of the Degree in

BACHELOR OF ARTS/ BACHELOR OF SCIENCE/HONOURS

(Offered under 4-year UG Degree Programme)

(Credit Based Grading System)
under NEP 2020

Batch: 2025–29

GURU NANAK DEV UNIVERSITY AMRITSAR

Skill Enhancement Courses in Computer Science
(CBGS) (under NEP 2020) (Batch 2025-29)

SCHEME

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES (SEC)

SEC-I

Sr. No.	Course Code	Course Title	Credits L - T - P	Total Marks
1.		INTRODUCTION TO THE INTERNET (THEORY)	2 - 0 - 0	50
2.		INTRODUCTION TO THE INTERNET (PRACTICAL)	0 - 0 - 1	25

SEC-II

Sr. No.	Course Code	Course Title	Credits L - T - P	Total Marks
1.		CYBER SECURITY FUNDAMENTALS (THEORY)	2 - 0 - 0	50
2.		CYBER SECURITY FUNDAMENTALS (PRACTICAL)	0 - 0 - 1	25

SEC-III

Sr. No.	Course Code	Course Title	Credits L - T - P	Total Marks
1.		SERVER-SIDE PROGRAMMING (THEORY)	2 - 0 - 0	50
2.		SERVER-SIDE PROGRAMMING (PRACTICAL)	0 - 0 - 1	25

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES

SEC-I

INTRODUCTION TO THE INTERNET

(THEORY)

M. Marks: 50 **Credits**
Time: 3 Hours **L-T-P**
2-0-0

Instructions for the Paper Setters: -
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

Course Outcomes:
To give hands-on experience and provide a comprehensive, non-technical, hands-on overview of the Internet based services.

SECTION–A

Origin, growth and evolution of the Internet; the impact of the Internet; terminology: web pages, website, web browser, web server, bandwidth; Connect to the Internet: hardware and software, types of the Internet connections, Internet Service Providers; Navigating different types of websites and online resources.

Student should explore the local market to understand the internet service providers, rates, bandwidth etc.

SECTION – B

E-mail Communication: E-mail Etiquette and Best Practices, Managing and Organizing E-mails E-mail Tools and Features, identifying spam and phishing E-mails;

Searching on the Internet: Overview of internet resources and search engines, Basics of Using Search Engines -How search engines work, Basic search techniques and tips, Understanding search engine results pages (SERPs), Using search operators (e.g., AND, OR, NOT), Utilizing advanced search features (e.g., Google Advanced Search),

SECTION - C

Online Tools for Productivity: Introduction to productivity tools (e.g., Google Workspace, Microsoft Office 365), Cloud storage and file management (e.g., Google Drive).

Collaboration and Communication Tools: Online communication etiquette and best practices, using collaboration tools (e.g., Google Docs, Slack, Microsoft Teams), Effective virtual meeting strategies (e.g., Zoom, Google Meet),

SECTION – D

Building Online Presence: Creating and maintaining a professional online profile (e.g., LinkedIn), Personal branding and digital portfolios, Networking strategies for academic and career growth, Understanding digital footprints and online reputation.

Digital citizenship and respectful online behaviour, balancing screen time and managing digital distractions

Recommended Books and Materials:

1. Douglas E Comer, The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works, CRC Press
2. Faithe Wempen, Digital Literacy For Dummies 1st Edition

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES

SEC-I

INTRODUCTION TO THE INTERNET

(PRACTICAL)

M. Marks: 25
Time: 3 Hours

Credits
L-T-P
0-0-1
Lab 2h/week

Instructions for the examiners: -

Two questions of equal marks strictly as per the syllabus and based on the practical exercises covered in the semester. Questions may be subdivided into parts (not exceeding four). Candidates will attempt ONE question, explain their answer by writing on the answer sheet, and then implement the same on the computer. Examiner will evaluate both the answers (theory as well as practical). The viva should also be conducted alongside, and the student is asked viva questions related to the question and the solution he/she is working on during the exam. Lab exercises based on:

- Identifying internet connections and Configuring internet connection on PC/Laptop
- E-mail Tools and features
- Using the Google search engine and explore Bing
- Using Google Docs, Google Drive for document preparation and storage
- Collaboration using Slack
- Analyzing LinkedIn profiles
- Creating your own LinkedIn profile
- Virtual meeting platforms: Microsoft Teams, Zoom, Google Meet

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES

SEC-II

CYBER SECURITY FUNDAMENTALS

(THEORY)

M. Marks: 50 **Credits**
Time: 3 Hours **L-T-P**
2-0-0

Instructions for the Paper Setters: -
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

Course outcome:

1. To teach fundamentals of Cyber Space, Cyber Threats and defense strategies,
2. understand the ethical, legal, and regulatory environment in the cyber space.

SECTION-A

Introduction to the Internet, IP address, MAC address; Client-Server/P2P Architecture, Cloud Computing; Computation/ Storage as a service; confidentiality, Integrity, availability of information; desktop and mobile apps; Authentication & authorization; Data trails of an Internet user; cookies; Why security matters?

SECTION-B

Threats: Malicious software, Cyber threats, hackers, trackers, types of hackers, hacker motives; Types of Attacks: virus, worms, Trojan horse, spam, spoofing, phishing, spear-phishing, whaling, social engineering, ransomware, spyware, adware, malvertising, supply-chain attacks, zero-day viruses - software/hardware vulnerabilities, exploits; denial of service attacks; bots, botnets; Data breaches; risks of using public Wi-Fi; Cyber bullying;

SECTION-C

How to Safeguard: Using http/https; Anti-virus software, analysis of the tools available in the market; strong passwords/passphrases, password managers, changing passwords regularly; Cryptography: Encryption, Decryption, public/private cryptography, Digital signatures; Virtual private networks; Setting up private and secure Wi-Fi; Data backup and recovery – full/incremental/differential backup, backup vs archive; software updates/patches; URL filtering;

SECTION-D

privacy vs security vs anonymity, privacy settings in apps/browsers and popular social networking sites such as Facebook, Instagram, Snapchat; using web browser incognito mode, the tor browser; Laws, regulations, and compliance; cybercrimes, Intellectual Property, Licensing, Compliance, Provisions in the IT act.

Reference Books:

1. Kenneth Einar Himma and Herman T. Tavani, Handbook of Information and Computer Ethics, Wiley.
2. Douglas E Comer, The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works, CRC Press
3. Introduction to cyber security: stay safe online, The Open University
4. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co. (ULPC)
5. Anirudh Rastogi, Cyber Law-Law Of Information Technology And Internet, Lexis Nexis
6. James Graham, Ryanolson Rickhoward, Cyber Security Essentials By, CRC PRESS
7. R. K. Dhamija, Cybersecurity: An Introduction, BPB Publications
8. Charles J. Brooks, Christopher Grow, and Philip Craig, Cybersecurity Fundamentals by McGraw-Hill

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES

SEC-II

CYBER SECURITY FUNDAMENTALS

(PRACTICAL)

M. Marks: 25
Time: 3 Hours

Credits
L-T-P
0-0-1
Lab 2h/week

Instructions for the examiners: -
Two questions of equal marks strictly as per the syllabus and based on the practical exercises covered in the semester. Questions may be subdivided into parts (not exceeding four). Candidates will attempt ONE question, explain their answer by writing on the answer sheet, and then implement the same on the computer. Examiner will evaluate both the answers (theory as well as practical). The viva will also be conducted one-on-one alongside, and the student asked viva questions related to the question and the solution he/she is working on during the exam.

Lab Exercises based on

- Find IP/MAC addresses on personal devices
- Set up a simple cloud service (e.g., Google Drive)
- Check browser cookies and understand privacy settings
- Conduct a phishing simulation to identify red flags
- Analyze secure connections, creation of strong passwords
- Configure a VPN on personal devices
- Data backup routine using a cloud service or external drive
- Adjust privacy settings on popular platforms like Facebook and Instagram
- Understand anonymity using Tor network
- Install and configure antivirus and anti-malware software
- Configure a firewall rule using pfSense or similar tools
- Use OpenSSL to encrypt and decrypt messages.

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES

SEC-III

SERVER-SIDE PROGRAMMING

(THEORY)

M. Marks: 50 **Credits**
Time: 3 Hours **L-T-P**
2-0-0

Instructions for the Paper Setters: -
Eight questions of equal marks (Specified in the syllabus) are to be set, two in each of the four Sections (A-D). Questions may be subdivided into parts (not exceeding four). Candidates are required to attempt five questions, selecting at least one question from each Section. The fifth question may be attempted from any Section.

SECTION-A

Introduction: Overview of web application architecture (client-server model), Difference between client-side and server-side programming, server-side programming and its role in web applications, Introduction to HTTP and web protocols

Setting Up the Development Environment: Installing and configuring a web server (e.g., Apache, Nginx),

Introduction to Programming Languages: Overview of server-side programming languages (e.g., Python, Node.js, Java, PHP), Choosing the right language for specific applications, Basics of syntax and structure of Python

Building a Simple Web Application: Setting up a basic web server (using Node.js/Express or similar), Handling HTTP requests and responses, Rendering dynamic content

SECTION-B

Working with Frameworks: Introduction to popular frameworks (Express for Node.js, Flask for Python, Spring for Java), Setting up a project using Flask for Python framework, Understanding the MVC (Model-View-Controller) architecture

RESTful API Development: Principles of REST architecture, Designing and implementing RESTful APIs, Handling CRUD operations with API endpoints

SECTION-C

Database Interaction: Connecting to databases (SQL and NoSQL), Performing CRUD operations with a database (using an ORM), Managing database migrations

Authentication and Authorization: Understanding user authentication and session management, Implementing authentication strategies (JWT, OAuth), Protecting routes and resources

Error Handling and Debugging: Common error types in server-side applications, Best practices for error handling, Debugging techniques and tools

SECTION-D

Web Security: Overview of common security vulnerabilities (SQL injection, XSS, CSRF), Implementing security measures (input validation, output encoding), Using HTTPS and securing APIs

Deployment and Hosting: Overview of cloud platforms (AWS, Heroku, Digital Ocean), Setting up and deploying a server-side application, Managing server resources and scaling applications

Recommended Textbooks:

1. David I. Schneider **"Server-Side Programming with Java: A Comprehensive Guide"** by
2. Miguel Grinberg **"Flask Web Development"** by Leonard Richardson and Sam Ruby**, RESTful Web APIs**
3. "WEB TECHNOLOGIES A Computer Science Perspective" by Jeffrey C. Jackson
4. "Learning PHP, MySQL & JavaScript: A Step-By-Step Guide to Creating Dynamic Websites" by Robin Nixon (BPB Publications)

COMPUTER SCIENCE

SKILL ENHANCEMENT COURSES

SEC-III

SERVER-SIDE PROGRAMMING

(PRACTICAL)

M. Marks: 25
Time: 3 Hours

Credits
L-T-P
0-0-1
Lab 2h/week

Instructions for the examiners: -
Two questions of equal marks strictly as per the syllabus and based on the practical exercises covered in the semester. Questions may be subdivided into parts (not exceeding four). Candidates will attempt ONE question, explain their answer by writing on the answer sheet, and then implement the same on the computer. Examiner will evaluate both the answers (theory as well as practical). The viva will also be conducted one-on-one alongside, and the student asked viva questions related to the question and the solution he/she is working on during the exam.

Lab Exercises based on:

- Setting Up a Flask Project and Implementing MVC Architecture in Flask
- Designing and Testing RESTful APIs
- Connecting to a SQLite or NoSQL Database and performing CRUD operations
- Implement user registration and login features using Flask-Login
- Use JWT for user authentication and Secure certain routes in the Flask application
- Best practices for error handling, Debugging techniques and tools
- Implementing security measures (input validation, output encoding), Using HTTPS and securing APIs
- Setting up and deploying a server-side application,
- Managing server resources and scaling applications