Re-Accredited 'B++' 2.86 CGPA by NAAC
VEER NARMAD SOUTH GUJARAT UNIVERSITY
University Campus, Udhna-Magdalla Road, SURAT - 395 007, Gujarat, India.
વીર નર્મદ દક્ષિણ ગુજરાત યુનિવર્સિટી
યુનિવર્સિટી કેમ્પસ, ઉધના-મગદલ્લા રોડ, સુરત - ૩૯૫ ૦૦૭, ગુજરાત, ભારત.
Tel : +91 - 261 - 2227141 to 2227146, Toll Free : 1800 2333 011, Digital Helpline No.- 0261 2388888
E-mail : info@vnsgu.ac.in, Website : www.vnsgu.ac.in

–: પરિપત્ર :–

યુનિવર્સિટી સંલગ્ન કોમ્પ્યુટર સાયન્સ વિદ્યાશાખા હેઠળની તમામ બીસીએ કોલેજોના આચાર્યશ્રીઓને જણાવવાનું કે, શૈક્ષણિક વર્ષ ૨૦૨૬–૨૭ થી અમલમાં આવનાર B.C.A. (Cyber Security and Data Protection) Sem.-5 & 6 નો પેટાસમિતિ દ્વારા તૈયાર કરવામાં આવેલ અભ્યાસક્રમ કોમ્પ્યુટર સાયન્સ વિષયની અભ્યાસ સમિતિના ચેરમેનશ્રીએ અભ્યાસ સમિતિવતી મંજૂર કરી કોમ્પ્યુટર સાયન્સ ફેકલ્ટીને કરેલ ભલામણ કોમ્પ્યુટર સાયન્સ ફેકલ્ટીની તા. ૨૯/૦૪/૨૦૨૬ ની સભાના ઠરાવ ક્રમાંકઃ૨૩ થી મંજૂર કરી એકેડેમિક કાઉન્સિલને કરેલ ભલામણ એકેડેમિક કાઉન્સિલની તા.૦૭/૦૫/૨૦૨૬ ની સભાનાં ઠરાવ ક્રમાંકઃ૬૧ થી મંજૂર કરેલ છે. જેનો અમલ કરવા આથી જાણ કરવામાં આવે છે.

બિડાણઃ ઉપર મુજબ

ક્રમાંકઃઓથો./પરિપત્ર/૧૦૦૩૮/૨૦૨૬
તા.૧૨/૦૫/૨૦૨૬

કુલસચિવ

પ્રતિ,

(૧) યુનિવર્સિટી સંલગ્ન તમામ બીસીએ કોલેજોના આચાર્યશ્રીઓ.
.....આપશ્રીની કોલેજ/વિભાગના સંબંધિત શિક્ષકો/વિદ્યાર્થીને જાણ કરી અમલ કરવા સારૂ.

(૨) ઈ.ચા.ડીનશ્રી, કોમ્પ્યુટર સાયન્સ વિદ્યાશાખા.

(૩) પરીક્ષા નિયામકશ્રી, પરીક્ષા વિભાગ, વીર નર્મદ દ. ગુ. યુનિવર્સિટી, સુરત.
.....તરફ જાણ તેમજ અમલ સારૂ.

Veer Narmad South Gujarat University, Surat

Computer Science and Information Technology Faculty

Syllabus for (Semester-V and Semester-VI) of B.C.A.(Cyber Security and Data Protection)

As per NEP-2020

To be implemented from

Academic Year: June, 2026-2027

Veer Narmad South Gujarat University, Surat
Bachelor of Computer Application ((Cyber Security and Data Protection) (Honours))
Under the Faculty of
Computer Science and Information Technology

Name of Program:	Bachelor of Computer Application (Cyber Security and Data Protection) (Honours)
Abbreviation:	B.C.A.(Honours): Four-year Integrated Program. With Multi-Level Entry and Exit option
Multi-level Exit Criteria:	i) Under Graduate Certificate in Computer Application: If the student wish to exit after completion of First year (Semester-1 and Semeter-2) without any back-log and secure additional 4 credits from work based skill oriented university approved courses /vocational courses / summer internship / Apprenticeship in addition to 6 credits from skill-based courses earned during first and second semester. ii) Diploma in Computer Application: If the student wish to exit after completion of Second year (Semester-1 to Semeter-4) without any back-log and secure additional 4 credits from work based skill oriented university approved courses /vocational courses / summer internship / Apprenticeship offered at end of first or second year in addition to 6 credits from skill-based courses earned during first four semesters. iii) B.C.A. (Bachelor's in Computer Application): If the student wish to exit after completion of Third year (Semeste-1 to semester-6) without any back-log and secure additional 4 credits from work based skill oriented university approved courses /vocational courses / summer internship / Apprenticeship offered at end of first or second year in addition to 6 credits from skill-based courses earned during first four semesters.
Multi-Level Entry Criteria:	As per the norms of the Veer Narmad South Gujarat University.
Duration:	3rd year of B.C.A.(Honors) degree program with multi-level exit options at 1st, 2nd and 3rd Year to obtain Certificate, Diploma, Degree and Honours Degree in Computer Application respectively.
Eligibility:	Candidate must have passed standard 12th (H.S.C.) Examination in Science (Any Group) / Commerce / vocational / General stream from Gujarat Higher Secondary Board (G.H.S.E.B.) or any other equivalent board (C.B.S.E. / I.C.S.E. / NIOS etc. which must be approved and possess equivalence certificate from Veer Narmad South Gujarat University) with English as one of the subject. In case of candidates passed out from 12th Board from General Stream; having English as one of the subjects. In case of Students passed out with 12th (H.S.C.) vocational stream, Computer and English must be one of the subject.
Objective of the Program:	Bachelor of Computer Application (Cyber Security and Data Protection) (Honours) is undergraduate degree program in computer application area. Objective of the program is to open a channel of admission for courses in the field of Computer Science,

	Applications and all relevant fields of information technologies to build career for students who have completed standard 12th (H.S.C.) and are interested in taking computing/computer Application and Information Technology as a career. Main objective is to equip the students with strong foundation in computer programming languages, coding, database handling, software application developments, problem-solving skills and development of analytical and logical skills. The focus is to introduce various programming languages on different platforms and operating systems, interaction with databases available on various platforms, software testing, and development and deployment techniques. It also aim to provide knowledge in latest trends and advancements in field of computer technologies. The program caters to the needs of the students aspiring to excel in the field of computer science, applications and technologies. The program is designed to develop computer professionals versatile in almost all field of computer application. It also aim to enhance communication and interpersonal skills.
Program Outcome:	**PO1:** Ability to analyze a problem, identify and define the Computing requirements appropriate to its solution. **PO2:** Enhancing the problem solving, logical, reasoning and analysis capabilities of a problem and integrate the ability with the coding using specific computer programming languages. **PO3:** To generate Understanding regarding the core and fundamental ideas about the computer platforms, operating systems, software design concepts, networking concepts and advanced and emerging technologies. **PO4:** Design, implement and evaluate a computer-based system, processing, component or program to meet desired goal with the help of various programming languages, application software, packages, tools, databases on various platforms. **PO5:** An ability to apply design and development principles in construction of software systems of varying complexity using various algorithmic principles, modeling, coding and design of computer-based systems. **PO6:** Prepare the aspiring students to become computer software professionals who can work in corporate/software industry at entry to advanced level as well as independent developers. Overall, the program outcomes aim to produce graduates who are: (a) competent in computer application, development and design. (b) Adapt to changing technology and industry trends. (c) Can make significant contributions to the software applications coding, designing, database managements, testing, deployments and ready to adapt any upcoming technologies.

Program Specific Outcome:	**PSO1:** Developing understanding about the fundamentals of core concepts of logic developments, critical thinking and problem solving capabilities. Emphasis on effective communication. **PSO2:** Improving analytical and applied concepts using various technologies, coding concepts and implementation of coding to solve the problems. **PSO3:** Development of team building concepts and working in team with positive approach, enhancing the mindset to contribute as an individual to the team. Improving interpersonal skills. **PSO4:** Improving student's Understanding related to technical problems and enhancing their capabilities to address the problems to turn into solutions through various possible ways by enhancing critical thinking ability. **PSO5:** Develop students to capabilities for self-learning, skill development through self-practicing and problem solving abilities. **PSO6:** Develop students to address and work on the real-world problems as an individual and as part of team. Understand the business problems and ability to work on their solutions by applying various software technologies. **PSO7:** To enhance development skills at various level including problem analysis, data analysis, logical and critical analysis of the problems and implementing the solutions by imparting various recent and upcoming technologies. **PSO8:** Enhance the passion among the students for updating knowledge, innovative ideas, upskilling and implementing the knowledge in applied areas and research areas by understanding the real world problems, addressing the real world problems and their possible solutions that lead to build a successful Professional career.
PO and PSO mapping:	
Medium of Instruction:	English
Program Structure:	Semester-wise Breakup of the course is given as follows :

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
PO1								
PO2								
PO3								
PO4								
PO5								
PO6								

Veer Narmad South Gujarat University, Surat

Program Structure: T.Y.B.C.A. (SEM – 5 and SEM – 6)

(w.e.f. Academic Year June, 2025-2026)

Bachelor of Computer Application (Cyber Security and Data Protection) (B.C.A.) – Three Year Program

Bachelor of Computer Application (Cyber Security and Data Protection) (B.C.A.(Hon.)) – Four Year Integrated Program

Program Structure	Semester-wise break up for the courses :

SEMESTER – 5

Course Code	**Course Title**	**Course Category**	**Level of Course**	**Course Credits**	**Teaching Hours/week**	
				Th.+Pra.	Theory	Practical/ Fieldwork /Project/ Internship
501	Linux Operating System (LOS) (Minor-04)	Minor Corse	200-299 Intermediate Level Course	4	3	2
502	Network Technology (Minor-05)	Minor Course	200-299 Intermediate Level Course	4	4	0
503-04	Advanced Network Defense and Security Architecture	Major Course	300-399 Advanced Courses	4	2	4
504-04	Malware Analysis and Reverse Engineering	Major Course	300-399 Advanced Courses	4	2	4
505-04	Cyber Laws, IT Governance and Risk Management	Major Course	300-399 Advanced Courses	4	2	4
	Project-01 (Based on course code: 503-04)	Project will be developed in group of maximum three students based on approved definition by the concerned faculty members. The project report will be submitted by the students regularly. The final evaluation will be based on Project presentation, E-report and viva-voce.				
	Project-02 (Based on course code: 503-04)	Project will be developed in group of maximum three students based on approved definition by the concerned faculty members. The project report will be submitted by the students regularly. The final evaluation will be based on Project presentation, E-report and viva-voce.				
	Project-03 (Based on course code: 505-04)	Project will be developed in group of maximum three students based on approved definition by the concerned faculty members. The project report will be submitted by the students regularly. The final evaluation will be based on Project presentation, E-report and viva-voce.				
	Practical (Based on Course Code:501)	Students will prepare separate practical journals for both courses. The final Practical exam/viva-voce will be based on 501 separately.				
506	Concept of HTML, CSS, Javascript and JQuery (SEC-05)	Skill Enhancement Course	200-299 Intermediate Level Course	2	2	-
Other Activities	The student is expected to participate in activities related to National Service Scheme (NCC), National Cadet Corps (NCC), adult education/literacy initiatives, mentoring school students, Elderly literacy program/ Environment preservation activities and other similar activities.			-	-	-
Total				22	15	14

Course Code	Course Title	Course Credit	University Exam Type	Exam Duration	External Marks	Internal Marks	Total Marks
501	Linux Operating System (LOS) (Minor-04) **	4	Theory/ Written : Practical :	1 Hours 2 Hours	25 25	25 25	100
502	Network Technology (Minor-05)	4	Theory/ Written	2 Hours	50	50	100
503-04	Advanced Network Defense and Security Architecture (Major-11-01)**	4	Theory/ Written : Project :	1 Hours 2 Hours	25 25	25 25	100
504-04	Malware Analysis and Reverse Engineering (Major-12)**	4	Theory/ Written : Project :	1 Hours 2 Hours	25 25	25 25	100
505-04	Cyber Laws, IT Governance and Risk Management ** (Major-13)	4	Theory/ Written : Project :	1 Hours 2 Hours	25 25	25 25	100
506	Concept of HTML, CSS, Javascript and JQuery (SEC-05)	2	-	-	25	25	50#
Total		22			275	275	550

For Practical and Project:

- Batch Size: Maximum 40 students can be accommodated in a batch. Separate batch should be considered if the student strength exceed 45 numbers.
- Practical includes Lab. sessions for course-501
- Project hours includes Lab. sessions of 2 Hours each for the course-503-04 and course 504-04 and 505-04 per week. The students can work on project in-house/out-house as per their internal guide's guidance. Group of maximum three students can work on a project definition. One Internal Project guide will be allocated to each group. Each group is expected to work minimum 4 hours each on Project-1 and Project-2 per week. Out of which 2 hours will be in supervised mode and balance hours in un-supervised mode.
- The Practical journal/Project final reports must be certified by the concerned faculty and by the Head of the Department, failing which the student will not be allowed to appear for External Practical/Project Examination. Student will submit softcopy of Project duly certified by the internal guide.

Internship: A student who wish to exit after successfully completion of Third year (Semester-5 and Semester-6) without any backlog is required to obtain Four credits at the end of the year either through the internship/field-work or university approved two skill based certificate courses(two courses of 2-credits each or one 4-credit course). Student is required to enrol for the certificate courses separately by paying the course fees as decided by the college/institute. For Internship, the Institute/college will grant the permission and evaluate the training outcomes. Based on satisfactory completion of the internship training, the Institute head will recommend to the university to grant four credits for summer training. [All expenses for the internship/skill course/field-work will be bear by the student.]

Skill Enhancement Course: As per NEP(National Education Policy-2020), it is mandatory for students to select a 2 credit skill enhancement course out of the choices given by the college/institute (From available basket of courses as per University norms) or 2-credit MOOCs approved by the KCG. It will be mandatory for the student to opt minimum one 2-credit Skill enhancement/2-credit KCG approved MOOCs courses out of offered courses recognised by University during semester-1 to semester-5.

(If a student chooses to pursue an SEC (Skill Enhancement Course) other than the one offered by the institute/college—which is a 2-credit course approved as per the norms of KCG and NEP-2020—they must enroll for it separately, fulfill all necessary requirements, and submit a valid completion certificate in order to earn the required SEC credits.)

 # Marks: : The students will enrol for the course from the given university approved list of certificate courses offered by the respective college/department. The student will select and enrol separately for any of the offered list of courses at college/department/institute and obtain respective credits. The institute will evaluate the performance (preferably continuous evolution) as per the SOP of certificate courses and on successfully completion of the course, the student will be eligible to obtain respective credits for the course. These credits will be considered and reflect in student's mark-sheet as well as in ABC(Academic Bank of Credit). These courses are mandatory and student is required to obtain the specified credits in process to acquire the certificate/diploma/degree.

** Minor/Major Practical based Subjects: Course 503-04,504-04 and 505-04 are 4-credit major courses consists of two components: Theory and Practical/Project. Course-501 is minor course and carry 4 credits consists of two components: Theory and Practical.

For Course-503-04 ,Coruse-504-04 and Course 505-04: 2 Hours of Theory and 4 hours of Project contact hours per week are allocated. For Course 501: 3 Hours of theory and 2 hours of practical per week are allocated.

Major courses carry 100 marks of exam weightage (50 theory and 50 practical/project). External and Internal distribution of marks are in ratio of 50:50 respectively. Students are required to acquire minimum passing marks from theory and practical collectively. Practical exams: For Course-501 (2 hours duration).

Project Exam: For course-503-04, Coruse-504-04 and 505-04– Separate project presentation and viva-voce will be conducted. External Theory/Practical/Project exam marks (25 marks each for course-501, course-503-04,504-04 and 505-04.) Division of marks for External Practical: Exam evaluation: 20 marks + Viva-voce: 5 Marks. Students are required to pass in both components (Theory and Practical/Project) collectively for course 501, 503-04, 504-04 and 505-04 as combined head (Theory + Practical/Project). It is mandatory for Students to appear for internal and external theory and practical exams for all courses. Similarly, In case a student remain absent in any of the component of Theory or Practical of minor/major course, the student will be considered fail.	
Program Passing Rules:	As per University rules.
Program Fees : (Per Semester) (One time fees and exam fees are additional as prescribed by the university) (w.e.f. Academic Year : 2026-27)	Semester Tuition Fees : As per norms of University Semester Laboratory Utilization fees : As per norms of University [Other one time /affiliation /exam fees, will be as per the norms of the University] [The fees for all certificate courses, Skill Enhancement Courses / Value Addition Courses; fees will be as per the prescribed limit for per credit as per the SOP of certificate courses decided by the university.]
Internal Marks Distribution :	For All Theory subjects (Out of 25) : Home Assignment (3 marks) + Class Assignment (3 Marks) + Attendance (4 Marks) + Internal Test (15 marks) For All Practical/Project subjects (Out of 25) : Lab. work (3 marks) + Lab. Journal (3 Marks) + Attendance (4 Marks) + Internal Test (15 marks) For All Theory subjects (Out of 50) : Home Assignment (6 marks) + Class Assignment (6 Marks) + Attendance (8 Marks) + Internal Test (30 marks) For All Practical/Project subjects (Out of 50) : Lab. work (6 marks) + Lab. Journal (6 Marks) + Attendance (8 Marks) + Internal Test (30 marks)

[Subject Code for theory- 2511000905044001]

[Subject Code for Practical-2511000905044002]

Course Code: 501
Course Title: Linux Operating System

Course Code	501
Course Title	Linux Operating System (LOS)
Credits	4
Course Category	Minor Course
Level of Course	200-299 (Intermediate Level)
Teaching per Week	4 Hrs. (3 Hours Theory + 2 Hours Practical work)
Minimum Hours/ Semester	45 hours of Theory + 15 Hours of Practical (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2025-2026
Purpose of Course	Learn the architecture and features of Linux systems. Get familiar with the Linux file system, processes, and user management. Use basic and advanced Linux commands for file manipulation, text processing, permissions, networking, etc., Navigate the file system, manage files/directories, and control user access.
Course Objective	1. Understand the structure, design, and usage of Linux systems. 2. Gain hands-on experience with commands for file handling, process control, text processing, and system management. 3. Learn how to write, debug, and execute shell scripts using Bash or other shells to automate tasks. 4. Understand file types, directory structures, permissions, and access control. 5. Concepts of background/foreground jobs. 6. Use standard input/output effectively for chaining commands and redirecting data streams. 7. Apply logic and scripting to solve practical problems and streamline system operations.
Pre-requisite	Understanding of operating systems, files, and general computer usage, Basic understanding of variables, loops, conditionals, and functions, Experience with any programming language (like C, Python, or Java) is helpful but not always required, Concepts like processes, memory, and file systems give a better context to Linux systems.
Course Outcomes	**CO1:** Understand: Explain the structure and components of Linux systems. **CO2:** Apply: Use Linux commands for file handling, text processing, and system tasks. **CO3:** Create: Write and execute shell scripts to automate operations. **CO4:** Analyze: Analyze file types, permissions, and directory structures. **CO5:** Apply: Use redirection and pipes to control input/output streams.

Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-			-		-	-
CO2			-	-		-	-	-
CO3		-	-		-	-		-
CO4	-	-		-	-		-	
CO5		-	-		-			

Course Content

Unit 1 : Introduction to Linux Operating System

1.1 Features of Linux OS
1.2 Components of Linux OS (Hardware, Kernel, Shell, GNU Utilities & Applications)
1.3 Shell in Linux (Bash, Zsh, Dash – Features and Differences)
1.4 Introduction to Files and File Types in Linux (text, binary, special files)
1.5 Linux Directory Structure and File System Hierarchy Standard (FHS)

Unit 2 : Basic Linux Commands
2.1 Directory Navigation Commands (pwd, cd, mkdir, rmdir, ls, tree)

	2.2 File Management Commands (cat, rm, cp, mv, touch) 2.3 File Permissions and Ownership (chmod, chgrp, chown, umask) 2.4 Common System Commands (who, whoami, man, echo, date, clear) 2.5 Text Processing Commands (head, tail, cut, sort, cmp, tr, uniq, wc, tee) 2.6 Introduction to Process 2.7 Process Control commands : ps, fg, bg, kill, sleep 2.8 Job Scheduling commands : at, batch, crontab **Unit 3 : Shell Scripting in Linux** 3.1 Creating and Executing Shell Scripts (nano, vi, ./script.sh) 3.2 Shell Metacharacters and Operators 3.2.1 Filename Expansion (wildcards: *, ?, []) 3.2.2 Input/Output Redirection (>, >>, <) 3.2.3 Pipes (|) 3.2.4 Command Substitution ($(...), ...) 3.3 Control Flow Structures (if-else, case, for, while, until) 3.4 Logical Operators (&&, ||, !) 3.5 test and [ ] command for Condition Testing (file, numeric, string) 3.6 Arithmetic Operations (expr, $(( ))) **Unit 4 : Advanced Text Processing Tools** 4.1 Introduction to Regular Expressions (Basic and Extended) 4.2 Pattern Matching using grep, egrep, and fgrep 4.3 Stream Editing with sed (search, replace, line deletion, insertion)
Reference Books	1. Operating System: Unix and Linux, Behrouz A. Forouzan and Richard F. Gilberg, Cengage India Pvt. Ltd., ISBN:9788131502980 2. UNIX Concepts and Applications, Sumitabha Das, McGraw Hill Education (India), ISBN:9781259006382 3. Introduction to UNIX and Shell Programming, M. G. Venkateshmurthy, Pearson Education India, ISBN:9788131704377 4. Linux Programming and Administration, N.B. Venkateswarlu, BPB Publications, ISBN:9788176567813 5. UNIX and Shell Programming, B.A. Forouzan & F. Gilberg, Cengage Learning India, ISBN:9788131508050 6. Linux Command Line and Shell Scripting Bible, Richard Blum and Christine Bresnahan, Wiley India Pvt. Ltd., ISBN:9788126562169 7. How Linux Works: What Every Superuser Should Know, Brian Ward, No Starch Press, ISBN:9781593275679 8. The Linux Programming Interface, Michael Kerrisk, No Starch Press, ISBN:9781593272203 9. Linux Pocket Guide, Daniel J. Barrett, O'Reilly Media, ISBN:9781491927571 10. UNIX and Linux System Administration Handbook, Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin, Pearson Education, ISBN:9780134277554
Teaching Methodology	Class Work, Discussion, Lab work, Self-Study, Seminars and/or Assignments
Evaluation Method	50% Internal assessment. - Attendance, Class and home Assignment, Unit tests. - Practical exam, viva-voce, E-Journal 50% External assessment. - Written Theory exam - Practical Exam, viva-voce

Course Code: 502
Course Title: Network Technology

Course Code	502
Course Title	Network Technology (Minor-5)
Credits	4
Course Category	Minor Course (Minor-05)
Level of Course	200-299 (Intermediate Level Course)
Teaching per Week	4 Hours
Minimum Hours per Semester	60 hours of Theory (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2025-2026
Purpose of Course	To provide students with a foundational understanding of computer networks, covering basic concepts, architectures, protocols, and services. It aims to equip learners with the knowledge of both traditional and emerging network technologies, including Internet, Intranet, and Mobile Ad hoc Networks (MANET), essential for careers in Computer and IT industries.
Course Objective	1) To introduce students to the fundamental concepts and types of computer networks and topologies. 2) To explain the architecture and functioning of the Internet and Intranet, including various networking devices and media. 3) To explore the structure and functions of the OSI model and important network protocols. 4) To provide knowledge of modern networking trends such as Mobile Ad hoc Networks (MANET), VANET, FANET, and SPANC. 5) To demonstrate the working of application layer services such as email communication and web access through case studies.
Pre-requisite	Learner should have a basic understanding of computer fundamentals and operating systems. Familiarity with hardware components and general internet usage will be beneficial for better comprehension of networking concepts.
Course Outcomes	**CO1** (Remembering & Understanding)**:** Identify and describe types of computer networks, topologies, and related terminologies. **CO2** (Understanding & Applying)**:** Explain the working of Internet and Intranet and identify common networking devices and cables. **CO3** (Understanding & Applying)**:** Describe Mobile Ad hoc Networks (MANET, VANET, SPANC, FANET) and explain the OSI model and its layers. **CO4** (Applying): Apply knowledge of networking protocols, data packets, and addressing schemes (IP, HTTP, HTTPS) in basic scenarios. **CO5** (Analyzing): Analyze the role of application layer services in email communication and URL structure. **CO6** (Evaluating & Creating): Evaluate how different network protocols function across layers and create logical interpretations of data flow in web and email transactions.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1	■	-	-	-	-	-	-	-
CO2	-	■	-	■	-	-	-	-
CO3	■	-	-	-	-	-	■	-
CO4	■	■	■	-	■	-	-	-
CO5	-	-	-	-	■	■	■	-
CO6	■	-	-	-	■	-	-	■

Course Content

Unit-1: Introduction to Network

1.1 Basics of network
- 1.1.1 Types of networks
- 1.1.2 Different topologies (Bus, ring, star, mesh, tree)

1.2 Types of networks (LAN, MAN, WAN)

1.3 Terminologies (Intranet, Internet, Unicast, Broadcast, Multicast)

Unit-2: Internet and Intranet

2.1 Concepts of Internet and Intranet
- 2.1.1 Working of Internet and its architecture
- 2.1.2 Working of Intranet and its architecture

	2.1.3 Network Devices terminologies: Hub, modem, switch, Routers, Gateways, Access point 2.2 Types of Cables: co-axial, UTP, Fiber Optic cable **Unit-3: Mobile Ad hoc network** 3.1 Concepts and types of MANET (Mobile Ad hoc network) 3.1.1 VANET (Vehicular Ad hoc Network) 3.1.2 Smart phone Ad hoc Network (SPANC) 3.1.3 Flying Ad hoc network (FANET) 3.2 concepts of OSI(Open Source Interconnection) layers 3.2.1 types of layers 3.2.2 Introduction of OSI Layers and their purpose: Physical layer, Data link layer and Network Layer, Transport layer and Session Layer. 3.3 Important protocols of Network layers 3.3.1 Concepts of Data packets and Datagram 3.3.2 Presentation layer protocols and their purpose: 3.3.2.1 SSL, HTTP, FTP, Telnet 3.3 Concepts of IP address 3.4 Difference between http and https **Unit-4: Mail Services** 4.1 Application Layer services: 4.1.1 concepts of email 4.1.2 working of email account and services 4.1.3 URL and URL types (Absolute, Relative) 4.2 Case study of email: 4.2.1 From sender to receiver (Mailer, Mail Server, Mailbox) 4.2.2 Functionality and use of protocols at different layers 4.3 Case study of locating Website: 4.3.1 URL and locating URL 4.3.2 Steps and protocols involved in accessing URL 4.3.3 Concepts of search engine and purpose.
Reference Books	1. Computer Networks**,** Andrew S. Tanenbaum, Pearson, ISBN: 9780132126953 2. Computer Networking: A Top-Down Approach, James F. Kurose & Keith W. Ross, Pearson, ISBN: 9780133594140 3. Data Communications and Networking, Behrouz A. Forouzan, McGraw-Hill Education, ISBN: 9780071326285 4. Computer Networking: Principles, Protocols and Practice, Olivier Bonaventure, Self-published, ISBN: 9780994000403 5. Computer Networks: A Systems Approach, Larry L. Peterson & Bruce S. Davie, Elsevier, ISBN: 9780123850591 6. Networking: A Beginner's Guide, Bruce Hallberg, McGraw-Hill Education, ISBN: 9780072226786 7. Data and Computer Communications, William Stallings, Pearson, ISBN: 9780133506488 8. Computer Networks and Internets, Douglas E. Comer, Pearson, ISBN: 9780136067416 9. Network Warrior, Gary A. Donahue, O'Reilly Media, ISBN: 9781449387866 10. High-Performance Browser Networking, Ilya Grigorik, O'Reilly Media, ISBN: 9781449344760
Teaching Methodology	Class Work, Discussion, Self-Study, Seminars and/or Assignments
Evaluation Method	50% Internal assessment. - Class attendance, class assignment, home assignment, Unit Tests. 50% External assessment. - Theory/Written examination

[Subject code for Theory-2611000905011007]

[Subject code for Practical-2611000905011008]

Course Code: 503-04

Course Title: Advanced Network Defense and Security Architecture

Course Code	503-04
Course Title	Advanced Network Defense and Security Architecture
Credits	4
Course Category	Major Course
Level of Course	300-399 (Higher level Course)
Teaching per week	2 Hours Theory + 4 Hours of applied Project work.
Minimum Hours per Semester	90 Hours (30 Hours Theory + 60 Hours of Project work/ applied work (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Cognitive Skills of the Course	This course aims to provide in-depth knowledge of advanced network defence mechanisms, enterprise security architecture, monitoring techniques, cloud security fundamentals, and compliance practices. The course builds upon prior knowledge of Network Security, Cryptography, Ethical Hacking, and Incident Response.
Course Objective	1. To understand advanced network defence strategies and architecture models. 2. To implement firewall, IDS/IPS, and enterprise security controls. 3. To learn secure routing, switching, and wireless protection mechanisms. 4. To understand cloud and virtualization security risks and controls. 5. To develop skills in security monitoring, compliance, and risk management.
Pre-requisite	• Network Security and Penetration Testing • Cryptography and Secure Communication • Ethical Hacking and Vulnerability Assessment • Incident Response and Digital Forensics
Course Outcomes	CO1: Design secure network architecture using defence-in-depth principles. CO2: Configure and manage enterprise firewall and IDS/IPS systems. CO3: Apply secure routing, switching, and wireless security techniques. CO4: Analyze cloud security risks and implement access control strategies. CO5: Perform network monitoring, risk assessment, and compliance evaluation.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

CO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-		-	-	-	-	-
CO2			-	-		-	-	-
CO3				-	-	-	-	-
CO4				-		-	-	-
CO5								

Course Content	1. **Advanced Network Security Architecture** 1.1 Security Architecture Principles 1.2 Defense in Depth Model 1.3 Network Segmentation and DMZ 1.4 Zero Trust Architecture (ZTA) 1.5 Secure Network Design & Hardening 1.6 Secure Baseline Configuration 1.7 Network Access Control (NAC) 1.8 Secure Infrastructure Planning 2. **Enterprise Firewall and IDS/IPS Management** 2.1 Types of Firewalls (Stateful, Proxy, NGFW) 2.2 Firewall Rule Configuration and Policy Design 2.3 Intrusion Detection & Prevention Systems 2.4 Log Analysis & Traffic Monitoring 2.5 Introduction to SIEM 2.6 Threat Detection Techniques 2.7 Secure Gateway Configuration 2.8 Hands-on Enterprise Security Tools 3. **Secure Routing, Switching & Wireless Security** 3.1 VLAN Security & Port Security 3.2 Router & Switch Hardening 3.3 Secure Routing Protocols 3.4 Wireless Encryption Standards (WPA2, WPA3) 3.5 Rogue Access Point Detection 3.6 VPN Technologies (IPSec, SSL VPN) 3.7 Remote Access Security 3.8 Network Device Monitoring 4. **Cloud & Virtualization Security** 4.1 Cloud Security Fundamentals 4.2 Service Models (IaaS, PaaS, SaaS) – Security View 4.3 Identity & Access Management (IAM) 4.4 Cloud Firewalls & Monitoring 4.5 Virtualization Security Risks 4.6 Container Security Basics 4.7 Data Protection in Cloud 4.8 Cloud Compliance Concepts **Suggested Practical Work** • Firewall configuration and rule implementation • IDS/IPS setup and traffic analysis • VLAN and port security configuration • VPN setup simulation • Cloud IAM configuration (concept-based lab)
Reference Books	1. **Network Security Essentials: Applications and Standards** – William Stallings – Pearson 2. **Network Security Bible** – Eric Cole – Wiley 3. **Zero Trust Networks** – Evan Gilman & Doug Barth – O'Reilly 4. **Applied Network Security Monitoring** – Chris Sanders & Jason Smith – Syngress 5. **Cloud Security and Privacy** – Tim Mather, Subra Kumaraswamy & Shahed Latif – O'Reilly 6. **The Practice of Network Security Monitoring** – Richard Bejtlich – No

	Starch Press 7. **Computer Security: Principles and Practice** – William Stallings & Lawrie Brown – Pearson
Teaching Methodology	Class Work, Case Study, Lab Work, Simulation, Security Tool Demonstration, Self-study, Assignments
Evaluation Method	50% Internal assessment. : - Attendance, Class and home Assignment, Unit tests. - Practical work, Application Development,Vice-voce 50% External assessment. : - Theory/Written examination - Project demonstration/presentation, viva-voce

[Subject code for Theory-2611000905022005]

[Subject code for Practical-2611000905022006]

Course Code: 504-04

Course Title: Malware Analysis and Reverse Engineering

Course Code	504-04
Course Title	Malware Analysis and Reverse Engineering
Credits	4
Course Category	Major Course
Level of Course	300-399 (Higher Level course)
Teaching per Week	2 Hours Theory + 4 Hours of practical
Minimum Hours per Semester	90 Hours
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	This course provides in-depth knowledge of malware behaviour, analysis techniques, reverse engineering fundamentals, and secure investigation methodologies. It enables students to analyse malicious software in controlled environments and prepare professional incident reports.
Course Objective	1. To understand malware types and attack techniques. 2. To perform static and dynamic malware analysis. 3. To learn reverse engineering fundamentals. 4. To analyse exploit techniques used in malware. 5. To prepare structured malware investigation reports.
Pre-requisite	• Network Security and Penetration Testing • Cryptography and Secure Communication • Ethical Hacking and Vulnerability Assessment • Digital Forensics & Incident Response • Basic Linux & Windows Concepts
Course Outcomes	CO1: Identify and classify different types of malware. CO2: Perform static malware analysis using appropriate tools. CO3: Conduct dynamic behavioural analysis in sandbox environments. CO4: Apply reverse engineering techniques to examine malicious code. CO5: Prepare professional malware investigation and incident reports.

Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)

CO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1			-	-	-	-	-	-
CO2				-	-	-	-	-
CO3					-	-	-	-
CO4						-	-	-
CO5						-	-	-

Course Content

1. Introduction to Malware and Threat Landscape

1.1 Introduction to Malware

1.2 Types of Malware (Virus, Worm, Trojan, Ransomware, Rootkit, Spyware)

1.3 Malware Lifecycle

1.4 Attack Vectors and Infection Techniques

1.5 Indicators of Compromise (IOC)

1.6 Advanced Persistent Threats (APT)

1.7 Case Studies of Major Malware Attacks

1.8 Ethical and Legal Considerations

2. Static Malware Analysis

	2.1 Static vs Dynamic Analysis 2.2 File Formats (PE Structure Overview) 2.3 Hash Analysis (MD5, SHA) 2.4 String and Header Analysis 2.5 Packers and Obfuscation Techniques 2.6 Digital Signature Verification 2.7 Introduction to Disassemblers 2.8 Basic Reverse Engineering Concepts **3. Dynamic Malware Analysis** 3.1 Setting up Secure Lab Environment (VM-Based) 3.2 Sandbox Analysis Concepts 3.3 Process and Service Monitoring 3.4 Registry and File System Monitoring 3.5 Network Traffic Analysis 3.6 Memory Analysis Basics 3.7 Behavioural Analysis Techniques 3.8 Persistence Mechanisms Detection **4. Malware Detection, Prevention & Reporting** 4.1 Antivirus & Endpoint Detection Mechanisms 4.2 Signature-based vs Behaviour-based Detection 4.3 Introduction to YARA Rules 4.4 Threat Intelligence Platforms 4.5 Incident Documentation & Reporting 4.6 Malware Analysis Report Writing 4.7 Legal Compliance in Malware Research 4.8 Emerging Trends (AI-driven Malware) **Suggested Practical Work** • Setting up isolated malware lab using Virtual Machines • Hash calculation and file inspection • Static string extraction and header analysis • Dynamic behaviour monitoring • Network traffic capture and analysis • Writing structured malware analysis report
Reference Books	1. **Practical Malware Analysis** – Michael Sikorski & Andrew Honig – No Starch Press 2. **The Art of Memory Forensics** – Michael Hale Ligh et al. – Wiley 3. **Malware Analyst's Cookbook** – Michael Hale Ligh et al. – Wiley 4. **Learning Malware Analysis** – Monnappa K A – Packt
Teaching Methodology	Lecture, Lab Work, Malware Simulation, Case Study, Tool Demonstration, Self-Study, Assignments

Evaluation Method	50% Internal assessment. : - Attendance, Class and home Assignment, Unit tests. - Practical, Application Development viva-voce 50% External assessment. : - Theory/Written examination - Project demonstration/presentation, viva-voce

[Subject code for Theory-*2611000905033005*]

[Subject code for Practical-*2611000905033006*]

Course Code: 505-04

Course Title: Cyber Laws, IT Governance and Risk Management

Course Code	505-04
Course Title	Cyber Laws, IT Governance and Risk Management
Credits	4
Course Category	Major Course
Level of Course	300-399 (Higher Level course)
Teaching per Week	2 Hours Theory + 4 Hours of Practical/ Case study
Minimum Hours per Semester	90 Hrs.
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	This course provides knowledge of cyber legal frameworks, regulatory compliance, IT governance standards, and risk management techniques required to manage organizational information security effectively. The course prepares students for roles in cyber compliance, IT audit, and governance domains.
Course Objective	1. To understand national and international cyber laws. 2. To study cyber crime investigation procedures and digital evidence handling. 3. To learn IT governance frameworks and compliance standards. 4. To apply risk assessment and mitigation strategies. 5. To develop skills in drafting IT security policies and audit reports.
Pre-requisite	• Introduction to Cyber Security • Ethical Hacking and Vulnerability Assessment • Incident Response and Digital Forensics • Basic Networking Concepts
Course Outcome:	CO1: Explain provisions of Indian cyber laws and IT Act. CO2: Analyze cyber crime cases and electronic evidence procedures. CO3: Apply risk assessment and mitigation techniques in organizations. CO4: Understand IT governance frameworks and compliance standards. CO5: Prepare IT policies, audit documentation, and compliance reports.

Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)

CO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1			-	-	-	-	-	-
CO2				-	-			-
CO3					-	-		
CO4						-	-	
CO5								

Course Content	1. **Introduction to Cyber Law & Indian Legal Framework** 1.1 Evolution of Cyber Law 1.2 Need for Cyber Legislation 1.3 Overview of Information Technology Act, 2000 1.4 IT (Amendment) Act, 2008 1.5 Digital Signatures & Electronic Records 1.6 Offenses and Penalties under IT Act 1.7 Cyber Appellate Tribunal 1.8 Role of Adjudicating Officers 2. **Cyber Crimes & Legal Investigation** 2.1 Types of Cyber Crimes (Hacking, Identity Theft, Phishing, Cyber Stalking, Cyber Terrorism) 2.2 Cyber Crime Investigation Process 2.3 Digital Evidence and Chain of Custody 2.4 Admissibility of Electronic Evidence 2.5 Role of Cyber Cell & CERT 2.6 Cyber Forensics in Legal Context 2.7 Case Studies of Major Cyber Crime Incidents 2.8 Reporting and Legal Documentation 3. **International Cyber Laws & Data Protection** 3.1 Global Perspective on Cyber Laws 3.2 Data Protection Principles 3.3 Overview of GDPR 3.4 Data Privacy Concepts 3.5 Cross-Border Data Transfer 3.6 Intellectual Property Rights in Cyber Space 3.7 Cyber Law in E-commerce & Social Media 3.8 Emerging Data Protection Regulations 4. **IT Governance, Risk Management & Security Planning (Practical Oriented)** 4.1 Introduction to IT Governance and Risk Management 4.2 IT Governance Frameworks Overview 4.3 Risk Identification and Classification 4.4 Risk Assessment Techniques 4.5 Risk Mitigation and Security Controls 4.6 Business Continuity and Disaster Recovery Planning 4.7 IT Security Policy Development and Documentation 4.8 Cyber Ethics and Professional Responsibility **Suggested Practical / Case Study Work** • Drafting Information Security Policy • Risk Assessment Matrix Preparation • Mock IT Audit Simulation • Compliance Checklist Preparation • Cyber Crime Case Analysis Report • Legal Documentation Preparation
Reference Book	1. **Cyber Law: Text and Cases** – Vakul Sharma 2. **Cyber Laws and IT Protection** – Harish Chander 3. **Information Technology Law and Practice** – Vakul Sharma 4. **IT Governance: How Top Performers Manage IT Decision Rights** – Peter Weill & Jeanne W. Ross – Harvard Business School Press

	5. **Information Security Management Principles** – Alan Calder & Steve Watkins 6. **Risk Management and Financial Institutions** – John C. Hull
Teaching Methodology	Lecture, Case Study, Legal Analysis, Policy Drafting Exercise, Group Discussion, Self-Study
Evaluation Method	50% Internal assessment. : - Attendance, Class and home Assignment, Unit tests. - Practical work, Application development, viva-voce 50% External assessment : - Theory/Written examination - Project examination, Presentation/viva-voce

[Subject code-2611000905060269]

Course code: 506

Course Title: Concept of HTML, CSS, Javascript and JQuery (SEC-05)

Course Code	506
Course Title	Concept of HTML, CSS, Javascript and JQuery
Credits	2
Course Category	Skill Enhancement Course
Level of Course	200-299 (Intermediate Level)
Teaching per Week	2 Hours (Any combination of Theory/Practical/Fieldwork/Project)
Minimum weeks per Semester	15 (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	• To introduce students to the fundamental concepts of web development and web technologies. • To develop skills for styling and formatting web pages using CSS. • To provide knowledge of JavaScript for creating dynamic and interactive web pages. • To understand the use of jQuery for simplifying JavaScript programming and DOM manipulation. • To develop the ability to build responsive and user-friendly websites. • To prepare students for further learning in advanced web development and modern web frameworks.
Course Objective	• To understand the basic structure and elements of HTML for creating web pages. • To learn CSS techniques for designing and formatting web page layouts. • To understand the fundamentals of JavaScript for adding interactivity to websites. • To develop skills in handling events, functions, and basic programming concepts in JavaScript. • To learn how to use jQuery for DOM manipulation and event handling. • To integrate HTML, CSS, JavaScript, and jQuery to develop dynamic and responsive web pages. • To build a foundation for advanced web technologies and modern web application development.
Pre-requisite	Basic Knowledge of Computer
Course Outcomes	1. Students will be able to **create structured web pages using HTML elements and attributes**. 2. Students will be able to **apply CSS to design and format web pages effectively**. 3. Students will be able to **use JavaScript to develop interactive and dynamic web pages**. 4. Students will be able to **implement control structures, functions, and events in JavaScript**. 5. Students will be able to **use jQuery for DOM manipulation and event handling**.

	6. Students will be able to **integrate HTML, CSS, JavaScript, and jQuery to develop functional websites**.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-	-	-	-		-	-
CO2			-	-		-	-	
CO3			-			-	-	
CO4						-	-	
CO5	-		-	-			-	
CO6	-	-	-					

Course Content

1. HTML Fundamentals and Page Structure

1.1 Introduction to Web Technology and HTML
1.2 Basic Structure of an HTML Document (<!DOCTYPE>, <html>, <head>, <body>)
1.3 HTML Elements, Tags and Attributes
1.4 Text Formatting Tags (Heading, Paragraph, Bold, Italic, Underline, Superscript, Subscript)
1.5 Creating Lists (Ordered List, Unordered List, Definition List)
1.6 Creating Hyperlinks and Anchor Tag
1.7 Working with Images (<img> tag and attributes)
1.8 Creating and Formatting Tables (Rows, Columns, Table Attributes)
1.9 HTML Forms and Form Controls (textbox, radio button, checkbox, submit button)
1.10 Semantic HTML Elements (<header>, <nav>, <section>, <footer>)

2. CSS Styling and Layout Technique

2.1 Introduction to CSS and its Advantages in Web Design
2.2 CSS Syntax, Selectors and Comments
2.3 Types of CSS (Inline, Internal, External)
2.4 CSS Color, Background and Font Properties
2.5 Styling Text (font-family, font-size, font-style, text-align, text-decoration)
2.6 CSS Box Model (Content, Padding, Border, Margin)
2.7 CSS Borders, Width, Height and Display Properties
2.8 Positioning Elements (Static, Relative, Absolute, Fixed)
2.9 CSS Float and Clear Properties
2.10 Introduction to Responsive Design and Media Queries

3. Core JavaScript Programming

3.1 Introduction to JavaScript and its Role in Web Development
3.2 JavaScript Syntax and Basic Structure
3.3 Variables and Data Types in JavaScript
3.4 JavaScript Operators (Arithmetic, Assignment, Comparison, Logical)
3.5 Conditional Statements (if, if-else, nested if, switch)
3.6 Looping Statements (for loop, while loop, do-while loop)
3.7 Functions in JavaScript (Declaration and Calling Functions)
3.8 Arrays and Basic Array Operations
3.9 JavaScript Events (onclick, onload, onmouseover)
3.10 Basic Input and Output (alert(), prompt(), console.log())

	4. jQuery – Unit: jQuery Fundamentals and DOM Manipulation 4.1 Introduction to jQuery and its Advantages over JavaScript 4.2 jQuery Setup and CDN Integration 4.3 jQuery Syntax and Selectors (ID, Class, Element selectors) 4.4 jQuery Events (click, dblclick, hover, keypress, submit) 4.5 jQuery Effects (hide, show, toggle, fadeIn, fadeOut, slideUp, slideDown) 4.6 DOM Manipulation Methods (html(), text(), val()) 4.7 jQuery CSS Manipulation (css() method) 4.8 jQuery Traversing (parent, children, siblings) 4.9 jQuery Animation (animate() method) 4.10 Introduction to jQuery AJAX
Reference Books	1. HTML5 Black Book: Covers CSS3, JavaScript, XML, AJAX, PHP and jQuery — Dreamtech Press 2. Mastering HTML, CSS & JavaScript Web Publishing — BPB Publications 3. Web Design with HTML, CSS, JavaScript and jQuery — Wiley 4. HTML & CSS: The Complete Reference — McGraw-Hill Education 5. JavaScript and jQuery: Interactive Front-End Web Development — Wiley 6. Web Programming: Building Internet Applications — Wiley 7. Web Technologies (HTML, JavaScript, CSS) — Oxford University Press India
Teaching Methodology	Class Work/ Discussion/Self-Study/ Seminars/Assignments/ Practical Training
Evaluation Method	50% Internal assessment. Class attendance, class assignment, home assignment, Unit Tests. 50% External assessment. Practical/Theory/Written examination

University Examinations

Course Code	Course	Exam Component	Max. Marks	Duration
501 (Minor-4)	Linux Operating System (LOS)	**Theory**	**25**	**1 Hours**
		Practical	**25**	**2 Hours**
502 (Minor-5)	Network Technology	**Theory**	**50**	**2 Hours**
503-04 (Major-11-01)	Advanced Network Defense and Security Architecture	**Theory**	**25**	**1 Hours**
		Project Presentation	**25**	**-**
504-04 (Major-12)	Malware Analysis and Reverse Engineering	**Theory**	**25**	**1 Hours**
		Project Presentation	**25**	**-**
505-04 (Major-13)	Cyber Laws, IT Governance and Risk Management	**Theory**	**25**	**1 Hours**
		Project Presentation	**25**	**2 Hours**
506 (SEC-05)	Skill Enhancement Course	**Theory/Practical**	**25**	Evaluation and Assessment will be carried out based on the nature of the course opted by Student.

Internship: Student willing to exit the program at the end of the two semesters and to avail the Certificate in Computer Application or exit the program at the end of the first four semesters and to avail the Diploma in Computer Application, it is essential to acquire four credits from internship. A key aspect of the internship is induction into actual work situations. Internships involve working with local industry, government or private organizations, business organizations, artists, crafts persons, and similar entities to provide opportunities for students to actively engage in on-site experiential learning. In option to these internships, the student can avail such four credits by availing two 2-credit university approved courses during any of these semesters. The student is required to enroll and avail these 4-credits and produce the evidence in process to opt the multi-level exit option after successfully completion of first year (two semester) or second year(four semesters).

SEMESTER – 6

Course Code	Course Title	Course Category	Level of Course	Course Credits	Teaching per week	
					Theory	**Practical/ Fieldwork/Project/ Internship**
601-01 (Minor-6-01) OR 601-02 (Minor-6-02) OR 601-03 (Minor-6-02)	E-Commerce & Cyber Security OR Concepts of A.I. and IoT Devices OR Computer Graphics (Student will opt any one minor course from the courses listed here)	Minor Course	200-299 Intermediate level	4	4	0
602-04 (Major-14)	Advanced Security Operations and Threat Hunting	Major Course	400-499 Advanced Courses	4	2	4
603-04 (Major-15-01)	Blockchain and Emerging Technologies Security	Major Course	400-499 Advanced Courses	4	2	4
604 (Major-16)	Project	Major Course	400-499 Advanced Courses	4	0	8
605	Project and Interview Presentation Soft Skills [Ability Enhancement Course] (AEC)	AEC	100-199 Foundation Course	2	0	2
606	INTERNSHIP	Internship	400-499 Advanced Course	4	-	120 hours of Supervised Applied work
Other Activities	The student is expected to participate in activities related to National Service Scheme (NCC), National Cadet Corps (NCC), adult education/literacy initiatives, mentoring school students, Elderly literacy program / Environment preservation activities and other similar activities.			-	-	-
Total				22	08	18

Course Code	Course Title	Course Credit	University Exam Type	Exam Duration	External Marks	Internal Marks	Total Marks
601-01 (Minor-6-01) OR 601-02 (Minor-6-02) OR 601-03 (Minor-6-02)	E-Commerce & Cyber Security OR Concepts of A.I. and IoT Devices OR Computer Graphics (Student will opt any one minor course from the courses listed here)	4	Theory/ Written :	2 Hours	50	50	100
602-04 (Major-14)	Advanced Security Operations and Threat Hunting **	4	Theory/Written: Practical/Project:	1 Hours 2 Hours	25 25	25 25	100
603-04 (Major-15-01)	Blockchain and Emerging Technologies Security **	4	Theory/ Written : Practical/Project :	1 Hours 2 Hours	25 25	25 25	100
604 (Major-16)	Project (Major-16) **	4	Project	4 Hours (In-house) + 4 Hours (External Project work)	50	50	100
605	Project and Interview Presentation Soft Skills [Ability Enhancement Course] (AEC)	2	Presentation / Seminar:	-	25	25	50
606	Internship	4	Internship Report presentation	-	50	50	100
Total		22			275	275	550

For Practical and Project:

- Batch Size – 40 Maximum (Desirable). Maximum 45 students can be accommodated in a batch. Separate batch should be considered if the student strength exceed 45 numbers.
- Practical includes Practical sessions for course-602-04 and course-603-04. **Minimum** 60 hours of Practical/Project hours each for course-602-04 and course-603-04 should be allocated per batch. Out of which 30 hours will be in supervised mode and balance hours in un-supervised mode.
- Students will create an application (in-house project) for course 602-04 and course-603-04 as project. Their practical/project assessment will be based on the mini-project(application) developed for the concerned courses 602-04 and course-603-04 in terms of demonstration, presentation and viva-voce. E-project report should be prepared by the students which must be certified by the concerned faculty and by the Head of the Department, failing which the student should not be allowed to appear for External Practical/project Examination. Student will submit softcopy of Minor Project duly certified by the internal guide.

Major Course : Major discipline is the main focus (Core) dominant subject and the degree will be awarded in that discipline. Students must secure a prescribed number of credits (50% of total credits) through core courses in the major discipline. Students can choose the courses from the pool of courses. The number of courses (subjects) in Major may vary from semester to semester.

Minor Course : Minor discipline is the broader understanding course beyond the major discipline course. It contains generic-electives for students to choose from the pool of courses. It helps students to gain broader knowledge in addition to relevant major disciplines courses as per their choices. Minor subjects may be from same or different disciplines. Student may make choices according to their interest/need, from ODL courses also.

Internship: A student who wish to exit after successfully completion of first year (Semester-1 and Semester-2) without any backlog is required to obtain Four credits at the end of the year either through the summer internship or university approved skill based certificate courses(two courses of 2-credits each or one 4-credit course). Student is required to enrol for the certificate courses separately by paying the course fees as decided by the college/institute. For summer training, the Institute/college will grant the permission and evaluate the training outcomes. Based on satisfactory completion of the summer training, the Institute head will recommend to the university to grant four credits for summer training. The Internship/summer training/skill based certificate courses will be an audit course.[The internship cost/fees will be bear by the student.]

Ability Enhancement Course (AEC): To be offered to students to achieve competency in a Modern Indian Language and English Language focused on language and communication skills. It may be a major specific course. The Credit allocated

for these courses is 10 credits of total credits for 3 years' bachelor's degree and four years' bachelor's degree programme. The courses can be selected by the college/institute from available basket of approved 2-credit certificate courses provided by the university.

Skill Enhancement Course : As per NEP(National Education Policy-2020), it is mandatory for students to select a 2 credit skill enhancement course out of the choices given by the college/institute (From available basket of courses as per University norms). It will be mandatory for the student to opt minimum one 2-credit Skill enhancement course out of offered courses recognised by University during semester-1 to semester-5.

(The student need to enrol separately and pay the fees as decided by the respective institute/department)

 # Marks: : The students will enrol for the course from the given university approved list of certificate courses offered by the respective college/department. The student will select and enrol separately for any of the offered list of courses at college/department/institute and obtain respective credits. The institute will evaluate the performance (preferably continuous evolution) as per the SOP of certificate courses and on successfully completion of the course, the student will be eligible to obtain respective credits for the course. These credits will be considered and reflect in student's mark-sheet as well as in ABC(Academic Bank of Credit). These courses are mandatory and student is required to obtain the specified credits in process to acquire the certificate/diploma/degree.

[The student is required to pay separately for these courses as prescribed by the college. The college will decide the fees for these courses based on the University norms/SOP for certificate course/credit fees.]

** Major Applied Subjects: Course 602-04 and 603-04 are major courses consists of two components: Theory and Practical/Project. These courses are carrying 4 credits.

For Course-602-04 : 30 hours of Theory and 60 hours of practical work per semester are allocated.

For Course 603-04 : 30 hours of Theory and 60 hours of practical work per semester are allocated.

Major courses carry 100 marks of exam weightage (50 theory and 50 project/practical). External and Internal distribution of marks are in ratio of 50:50 respectively. Students are required to acquire minimum passing marks from theory and practical collectively.

Project viva-voce for course-602-04, course-603-04 will be conducted.

External Theory and Practical/Project exam marks (25 marks each for course-602-04, course-603-04

Division of marks for External Project course-602-04, course-603-04 :

Project Demonstration and presentation evaluation: 20 marks + Viva-voce: 5 Marks.

Internal and External Major-Project Presentation (Course-604) : 50 Marks (Presentation/Code explanation/project Demonstration)

Project Demonstration and presentation evaluation: 35 marks + Viva-voce: 10 Marks + Project E-Documentation : 5 Marks

Students are required to pass in both components (Theory and Practical/Project) collectively for course 602-04,603-04 as combined head (Theory + Practical) for each major course. It is mandatory for Students to appear for internal and external theory and practical exams for all courses. Similarly, In case, a student remain absent in any of the component of Theory or Practical of particular major subject, the student will be considered fail for that particular major subject.

[It is recommended to complete the theory exams of 601 to 603 between

Program Passing Rules:	As per University rules.
Program Fees : (Per Semester) (One time fees and exam fees are additional as prescribed by the university) (w.e.f. Academic Year : 2026-27)	Semester Tuition Fees : As per the norms of University Semester Laboratory Utilization fees : As per norms of University [Other one time /affiliation /exam fees, will be as per the norms of the University] [For all certificate course fees, Skill Enhancement Courses and Value Addition Courses fees will be as per the prescribed limit for per credit as per the SOP of certificate courses decided by the university.]

[Subject code-2611000906044001]

Course Code: 601-01
Course Title: E-commerce and Cyber Security

Course Code	601-01
Course Title	**E-Commerece and Cyber Security (Minor-601-01)**
Credits	4
Course Category	Minor Course
Level of Course	200-299 (Intermediate Level)
Teaching Hours	60 Hours
Minimum Hours/ Semester	60 hours of Theory (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	This course aims to introduce students to the fundamental principles of electronic commerce and essential concepts of cyber security. It prepares learners to understand online transaction models, digital payment systems, and safeguards against cyber threats.
Course Objective	1. To understand the concepts, structure, and applications of e-Commerce and m-Commerce. 2. To study the infrastructure and network components that support online commerce. 3. To learn about various electronic payment systems and associated security mechanisms. 4. To identify and analyze different types of cybercrimes and their technical aspects. 5. To comprehend basic cyber security concepts and terminologies related to internet protocols. 6. To explore common cyberattacks, vulnerabilities, and the roles of different types of hackers.
Pre-requisite	Basic understanding of computer fundamentals, internet technologies, and networking concepts is recommended. Familiarity with web applications and general IT awareness will be beneficial.
Course Outcomes	**CO1:** Understand the fundamental concepts and framework of e-Commerce and m-Commerce. **CO2:** Explain the network infrastructure, payment methods, and associated security issues in e-Commerce. **CO3:** Identify various types of cybercrimes and their technical aspects. **CO4:** Describe key concepts, terminologies, and threats related to cyber security. **CO5:** Differentiate between types of hackers and understand common system vulnerabilities.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-			-		-	-
CO2			-	-		-	-	-
CO3		-	-		-	-		-
CO4	-	-		-	-		-	
CO5		-	-		-			

Course Content	**Unit 1: Introduction to Electronic Commerce** 1.1 Concepts of e-Commerce 1.2 Aims of e-Commerce 1.3 e-Commerce Framework 1.4 e-Commerce Consumer Applications 1.5 e-Commerce Organizational Applications 1.6 Introduction to m-Commerce

	Unit 2: Network Infrastructure of e-Com , Payment and Security: 2.1. Concepts of Information Way 2.2. Components of I-Way 2.2.1. Network Access Equipment 2.2.2. Local on-ramps 2.2.3. Global Information Distribution Network 2.3. Transaction Models 2.4 e-Commerce Payments and Security Issues 2.4.1. e-Commerce Payment Systems 2.4.2. Debit Card Based, Credit Card Based ,. Risks & EPS 2.4.3. e-Cash, e-Cheque, e-wallet 2.5. Security on Web, SSL **Unit-3: Introduction to Cyber Crimes:** 3.1 Category of Cyber Crimes 3.2 Technical Aspects of Cyber Crimes 3.2.1 Unauthorized access & Hacking 3.2.2 Trojan, Virus and Worm Attacks 3.2.3 E-Mail related Crimes: Spoofing, Spamming, Bombing 3.2.4 Denial of Service Attacks 3.2.5 Distributed Denial of Service Attack 3.3 Various crimes : 3.3.1 IPR Violations (Software piracy, Copyright Infringement, Trademarks Violations, Theft of Computer source code, Patent Violations) 3.3.2 Cyber Squatting, Cyber Smearing, Cyber Stacking 3.3.3 Financial Crimes: (Banking, credit card, Debit card related) **Unit-4: Cyber Security Fundamentals:** 4.1 Concepts of Cyber Security: 4.1.1 Types of Threats 4.1.2 Advantages of Cyber Security 4.2 Basic Terminologies: 4.2.1 IP Address, MAC Address 4.2.2 Domain name Server(DNS) 4.2.3 DHCP, Router, Bots 4.3 Common Types of Attacks: 4.3.1 Distributed Denial of Service 4.3.2 Man in the Middle, Email Attack 4.3.3 Password Attack, Malware 4.4 Hackers: 4.4.1 Various Vulnerabilities: 4.4.1.1 Injection attacks, Changes in security settings 4.4.1.2 Expouser of Sensitive Data 4.4.1.3 Breach in authentication protocol 4.4.2 Types of Hackers: White hat and Black hat [All Units carry Equal Weightage]
Reference Books	1. Frontiers of Electronic Commerce, Ravi Kalakota and Andrew Whinston, Addition Wesley 2. Electronic Commerce: A Managerial Perspective, Efraim turban, Jae Lee, David King, H. Michel Chung, Addition Wesley 3. E-Commerce: An Indian Perspective, Joseph, PHI 4. E-Mail Hacking, Ankit Fadia, Vikas Publishing House Pvt. Ltd. 5. e-Commerce Concept, Models Strategies, G.V.S. Murthy, Himalaya Publisher 6. Cyber Crime in India, Dr M Dasgupta, Centax Publications Pvt Ltd 7. Cyber Laws and Crimes, Barkha U, Rama Mohan, Universal Law Publishing Co. Pvt Ltd. 8. Cyber Crime, Bansal S.K., A.P.H. Publishing Corporation 9. Cyber Security Understanding Cyber Crime, Computer Forensic and Legal Perspectives, Nina Godbole, Sunit Belapur, Willey India Publication

Teaching Methodology	Class Work, Discussion, Presentation, Self-Study, Seminars and/or Assignments
Evaluation Method	50% Internal assessment. - Attendance, Class and home Assignment. - Unit Tests 50% External assessment. - Written Theory exam

[Subject code-2611000906044002]

Course Code: 601-02
Course Title: Concepts of A.I. and IoT Devices

Course Code	601-02
Course Title	**Concepts of A.I. and IoT Devices (Minor-6-02)**
Credits	4
Course Category	Minor Course
Level of Course	200-299 (Intermediate Level)
Teaching Hours	60 Hours
Minimum Hours/ Semester	60 hours of Theory (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	The purpose of this course is to provide students with a foundational understanding of Artificial Intelligence (AI) and the role of Internet of Things (IoT) devices in enabling AI applications. It aims to introduce key concepts, tools, and real-life integrations of AI and IoT, preparing students for further learning or project-based exploration in this emerging interdisciplinary field.
Course Objective	1) To introduce the basic concepts and history of Artificial Intelligence (AI). 2) To explain key AI techniques such as search algorithms, machine learning, and expert systems. 3) To familiarize students with IoT devices and their architecture. 4) To explore how IoT devices collect and transmit data for AI applications. 5) To discuss real-world use cases integrating AI with IoT in domains like healthcare, agriculture, and smart cities. 6) To encourage understanding of the challenges and future scope of AI-enabled IoT systems.
Pre-requisite	Basic knowledge of computer fundamentals and an introductory understanding of programming or logic-building concepts is recommended. No prior experience with AI or IoT is required.
Course Outcomes	**CO-1 Remembering:** Recall and define key concepts, history, and types of Artificial Intelligence and IoT technologies. **CO-2 Understanding:** Explain the architecture, components, and connectivity methods of IoT systems used in AI applications. **CO-3 Applying:** Apply AI algorithms to process real-time data collected from IoT devices for smart decision-making. **CO-4 Analyzing:** Analyze challenges related to data quality, latency, power consumption, and security in AIoT systems. **CO-5 Creating:** Design and present innovative AIoT solutions based on case studies and group collaboration.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-			-		-	-
CO2			-	-		-	-	-
CO3		-	-		-	-		-
CO4	-	-		-	-		-	
CO5		-	-		-			

Course Content	**Unit 1: Basics of Artificial Intelligence (AI)** 1.1 Introduction to Artificial Intelligence 1.2 History and Evolution of AI 1.3 Types of AI – Narrow, General, Super AI 1.4 Key Concepts: Machine Learning, Deep Learning, Natural Language Processing 1.5 Real-life Applications of AI in Various Sectors (Healthcare, Education, Agriculture, Manufacturing) **Unit 2: IoT Devices that Can Be Used in AI Applications – Basics**

	2.1 Introduction to Internet of Things (IoT) 2.2 Architecture of IoT Systems – Sensors, Actuators, Gateways, Cloud 2.3 Types of IoT Devices Useful in AI Projects 2.3.1 Environmental Sensors (Temperature, Humidity, Air Quality) 2.3.2 Motion and Position Sensors (Accelerometers, Gyroscopes, PIR) 2.3.3 Wearables and Smart Health Devices 2.3.4 Cameras and Microphones for Image and Voice Input 2.4 Basics of Connectivity: Wi-Fi, Bluetooth, Zigbee, LoRaWAN 2.5 Data Flow: From Sensors to AI Processing **Unit 3: Advanced Integration of AI with IoT** 3.1 Introduction to AIoT (Artificial Intelligence of Things) 3.2 Real-Time Data Processing Using AI Algorithms 3.3 Edge Computing vs Cloud AI in IoT 3.4 AI-Based Decision Making from IoT Inputs (examples: Smart Home, Smart Agriculture) 3.5 Challenges in AIoT: Data Quality, Latency, Power Consumption 3.6 Privacy, Security, and Ethical Considerations in AIoT **Unit 4: Summary and Case Study Discussion** 4.1 Summary of Key Concepts from AI and IoT 4.2 Case Study 1: Smart Farming using IoT and AI 4.3 Case Study 2: AI-Powered Smart Home Automation 4.4 Open Discussion on AIoT Trends and Future Scope 4.5 Group Activity: Analyze and Present an AIoT Use Case [All Units carry Equal Weightage]
Reference Books	1. Frontiers of Electronic Commerce, Ravi Kalakota and Andrew Whinston, Addition Wesley 2. Electronic Commerce: A Managerial Perspective, Efraim turban, Jae Lee, David King, H. Michel Chung, Addition Wesley 3. E-Commerce: An Indian Perspective, Joseph, PHI 4. E-Mail Hacking, Ankit Fadia, Vikas Publishing House Pvt. Ltd. 5. e-Commerce Concept, Models Strategies, G.V.S. Murthy, Himalaya Publisher 6. Cyber Crime in India, Dr M Dasgupta, Centax Publications Pvt Ltd 7. Cyber Laws and Crimes, Barkha U, Rama Mohan, Universal Law Publishing Co. Pvt Ltd. 8. Cyber Crime, Bansal S.K., A.P.H. Publishing Corporation 9. Cyber Security Understanding Cyber Crime, Computer Forensic and Legal Perspectives, Nina Godbole, Sunit Belapur, Willey India Publication
Teaching Methodology	Class Work, Discussion, Presentation, Self-Study, Seminars and/or Assignments
Evaluation Method	50% Internal assessment. - Attendance, Class and home Assignment - Unit Tests 50% External assessment. - Written Theory exam

[Subject code-2611000906044003]

Course Code: 601-03
Course Title: Computer Graphics

Course Code	601-03
Course Title	**Computer Graphics (Minor-6-03)**
Credits	4
Course Category	Minor Course
Level of Course	200-299 (Intermediate Level)
Teaching Hours	60 Hours
Minimum Hours/ Semester	60 hours of Theory (Including class work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	The purpose of the Computer Graphics course is to introduce students to the fundamentals of graphical systems, display technologies, and graphic standards. It enables students to apply algorithms and geometric transformations to create and manipulate basic graphical objects.
Course Objective	1) Define the key concepts, application areas, and file formats used in computer graphics. 2) Explain the working principles of various video display devices and scanning techniques. 3) Apply line drawing algorithms to generate basic graphic primitives like lines and circles. 4) Analyze the effects of geometric transformations such as scaling, rotation, translation, reflection, and shearing. 5) Create simple graphic designs by integrating graphical objects and transformation techniques.
Pre-requisite	The prerequisite for the Computer Graphics course is a basic understanding of programming concepts and mathematical foundations such as coordinate geometry and matrix operations.
Course Outcomes	**CO-1:**Remembering**:** Recall the application areas, file formats, and graphic standards used in computer graphics systems. **CO-2:**Understanding**:** Describe the architecture and functioning of various display devices, scan methods, and graphic object types. **CO-3:Applying:** Implement standard line drawing algorithms such as DDA and Bresenham for rendering basic graphic primitives. **CO-4:Analyzing:** Analyze the behavior and effects of geometric transformations like scaling, rotation, translation, reflection, and shearing on 2D objects. **CO-5:Creating:**Construct and manipulate graphical objects by integrating transformations and rendering techniques for simple graphic applications.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-			-		-	-
CO2			-	-		-	-	-
CO3		-	-		-	-		
CO4	-	-		-	-		-	
CO5		-	-		-			

Course Content	**Unit 1. Introduction** 1.1 Application areas of Graphics Systems 1.1.1. Presentation Graphics 1.1.2. Entertainment 1.1.3. Education and Training 1.1.4. Image Processing 1.2 Computer Graphics Files 1.3 Introduction to graphic standards **Unit 2. Graphics Systems** 2.1. Video Display Devices

	2.1.1. Refresh CRT 2.1.2. Color CRT 2.1.3. LCD 2.1.4. Direct View Storage Tube 2.2. Raster scan and Random Scan Display 2.3. Raster Graphics and Vector Graphics 2.4. Concepts of various objects: Point, Line, Circle, Ellipse and Polygons **Unit 3. Line generation** 3.1. Geometry of line 3.2. Frame Buffer 3.3. Line Drawing Algorithms 3.3.1. DDA Algorithm 3.3.2. VECGEN 3.3.3. Bresnahan 3.4. Line Styles 3.4.1. Thick line 3.4.2. Line caps and joint **Unit 4. Geometric Transformations** 4.1 Basic Transformations 4.1.1 Scaling 4.1.2 Translation 4.1.3 Rotation 4.1.3.1 Rotation about origin 4.1.3.2 Rotation about Homogeneous Coordinates 4.2 Other transformations 4.2.1 Reflection 4.2.2 Shearing [All Units carry Equal Weightage]
Reference Books	1. Computer Graphics - second edition, Donald Hearn & M. Pauline Baker – Tata McGraw Hill Pub. 2. Computer Graphics, Harrington S. -Tata McGraw Hill. 3. Computer Graphics, Desai A. A. –PHI. 4. Computer Graphics: Algorithms & Implementations, Mukherjee & Jana – PHI. 5. Interactive Computer Graphics, Giloi W. K. –Prentice Hall India. 6. Principles of Interactive Computer Graphics, New Man W. & Sproul P. F. –McGraw Hill 7. Procedural Elements for Computer Graphics, Rogers D. F. – McGraw Hill.
Teaching Methodology	Class Work, Discussion, Presentation, Self-Study, Seminars and/or Assignments
Evaluation Method	50% Internal assessment. - Attendance, Class and home Assignment - Unit Tests 50% External assessment. - Written Theory exam

[Subject code for Theory-2711000906011004]

[Subject code for Practical-2711000906011005]

Course Code: 602-04

Course Title: Advanced Security Operations and Threat Hunting

Course Code	602-04
Course Title	Advanced Security Operations and Threat Hunting
Credits	4
Course Category	Major Course
Level of Course	400-499 (Advance Level)
Teaching Hours	2 Hours Theory + 4 Hours Practical
Minimum Hours/ Semester	90 Hours
Review / Revision	-
Implementation Year:	A.Y. 2026-27
Purpose of Course	This course provides advanced knowledge of Security Operations Center (SOC) activities, threat detection, log analysis, threat hunting techniques, and incident response coordination. It prepares students for real-world SOC Analyst and Threat Intelligence roles.
Course Objective	1. To understand SOC architecture and operational workflow. 2. To analyse logs and detect security incidents. 3. To apply threat hunting methodologies. 4. To study threat intelligence frameworks. 5. To integrate detection, response, and mitigation strategies. 6.
Pre-requisite	• Network Security and Penetration Testing • Ethical Hacking and Vulnerability Assessment • Incident Response & Digital Forensics • Malware Analysis • Advanced Network Defense
Course Outcomes	CO1: Explain SOC structure and operational processes. CO2: Analyse system and network logs for threat detection. CO3: Apply threat hunting methodologies using security frameworks. CO4: Use SIEM tools for monitoring and incident correlation. CO5: Prepare incident response documentation and mitigation strategies.

Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)

CO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-		-	-		-	-
CO2				-	-		-	-
CO3						-		
CO4	-	-	-			-		
CO5	-					-	-	-

Course Content

1. **Security Operations Center (SOC) Fundamentals**
   - 1.1 Introduction to SOC
   - 1.2 SOC Architecture and Components
   - 1.3 Roles and Responsibilities in SOC
   - 1.4 Security Monitoring Lifecycle
   - 1.5 Alert Management Process
   - 1.6 Incident Classification & Prioritization

	1.7 SOC Metrics and Reporting 1.8 SOC Maturity Models **2. Log Management and SIEM** 2.1 Importance of Log Collection 2.2 Types of Logs (System, Network, Application, Security) 2.3 Log Correlation Concepts 2.4 Introduction to SIEM 2.5 Event Correlation and Alert Generation 2.6 Dashboard and Reporting 2.7 Use Cases Development 2.8 Hands-on Concepts with Open-Source SIEM **3. Threat Intelligence & Threat Hunting** 3.1 Threat Intelligence Concepts 3.2 Types of Threat Intelligence (Strategic, Tactical, Operational) 3.3 Indicators of Compromise (IOC) 3.4 MITRE ATT&CK Framework Overview 3.5 Threat Hunting Methodologies 3.6 Hypothesis-driven Hunting 3.7 Threat Intelligence Platforms 3.8 Reporting & Documentation **4. Advanced Incident Detection & Response** 4.1 Incident Detection Techniques 4.2 Attack Lifecycle (Cyber Kill Chain) 4.3 Endpoint Detection & Response (EDR) 4.4 Network Traffic Analysis 4.5 Malware Indicators Detection 4.6 Incident Escalation Procedures 4.7 Containment & Eradication Strategies 4.8 Post-Incident Review **Suggested Practical Work** • Log analysis and filtering exercises • SIEM dashboard monitoring simulation • Threat hunting case study • IOC detection and correlation • Incident response simulation exercise • Preparation of SOC incident report
Reference Books	1. Applied Network Security Monitoring – Chris Sanders & Jason Smith 2. The Practice of Network Security Monitoring – Richard Bejtlich 3. Blue Team Handbook: Incident Response Edition – Don Murdoch 4. Threat Hunting: A Practical Guide – Robbie Lee 5. Cybersecurity Operations Handbook – John C. Allen & Gary C. Kessler 6. Security Operations Center: Building, Operating, and Maintaining your SOC – Joseph Muniz & Gary McIntyre
Teaching Methodology	Lecture, Lab Work, Log Analysis Practice, Threat Hunting Simulation, Case Study, Tool Demonstration

Evaluation Method	50% Internal assessment. - Attendance, Class and home Assignment, Unit tests. - Practical work, Application Development, Viva-voce. 50% External assessment. - Theory / written examination - project presentation and demonstration, viva-voce

[Subject code for Theory-2711000906022006]

[Subject code for Practical-2711000906022007]

Course Code: 603-04

Course Title: Blockchain and Emerging Technologies Security

Course Code	603-04
Course Title	Blockchain and Emerging Technologies Security
Credits	4
Course Category	Major Course
Level of Course	400-499(Advance level)
Teaching per Week	2 Hours Theory + 4 Hours of Project work
Minimum Teaching Hours per Semester	90 Hours (Theory + Project work)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Cognitive Skills of the Course	This course provides knowledge of blockchain technology, cryptocurrency security, smart contract vulnerabilities, IoT security, and emerging cyber threats. It prepares students to understand modern decentralized systems and secure next-generation technologies.
Course Objective	1. To understand blockchain architecture and cryptographic foundations. 2. To study smart contracts and their security risks. 3. To analyse cryptocurrency threats and wallet security. 4. To learn IoT and cloud security challenges. 5. To explore emerging technologies and future cyber risks.
Pre-requisite	• Cryptography and Secure Communication • Network Security • Ethical Hacking • Malware Analysis • Security Operations
Course Outcomes	CO1: Explain blockchain architecture and consensus mechanisms. CO2: Identify smart contract vulnerabilities and security risks. CO3: Analyse cryptocurrency threats and wallet protection methods. CO4: Evaluate IoT and cloud-based security challenges. CO5: Assess emerging technologies and future cybersecurity trends.

Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)

CO / PSO	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1	-		-	-	-	-	-	-
CO2		-			-		-	-
CO3					-		-	
CO4			-	-		-	-	
CO5	-	-	-	-		-	-	

Course Content	**1. Fundamentals of Blockchain Technology** 1.1 Introduction to Blockchain 1.2 Distributed Ledger Technology (DLT) 1.3 Cryptographic Hash Function 1.4 Public & Private Key Cryptography 1.5 Blocks, Transactions & Merkle Trees 1.6 Consensus Mechanisms (PoW, PoS) 1.7 Public vs Private Blockchain 1.8 Blockchain Applications **2. Cryptocurrency & Wallet Security** 2.1 Introduction to Cryptocurrency 2.2 Bitcoin Architecture Overview 2.3 Cryptocurrency Transactions 2.4 Wallet Types (Hot & Cold Wallets) 2.5 Cryptocurrency Attacks (51% Attack, Double Spending) 2.6 Exchange Vulnerabilities 2.7 Private Key Protection 2.8 Regulatory and Legal Aspects **3. Smart Contracts & Security Risks** 3.1 Introduction to Smart Contracts 3.2 Ethereum Overview 3.3 Smart Contract Lifecycle 3.4 Common Smart Contract Vulnerabilities 3.5 Reentrancy Attack 3.6 Integer Overflow & Underflow 3.7 Secure Coding Practices 3.8 Smart Contract Audit Basics 4. **IoT, Cloud Security & Emerging Technologies** 4.1 Introduction to IoT Architecture and Cloud Integration 4.2 IoT Threat Landscape and Device Vulnerabilities 4.3 Secure Communication in IoT Systems 4.4 IoT Botnets and Large-Scale Cyber Attacks 4.5 Cloud Security Challenges in IoT Environments 4.6 Edge Computing Security and Risk Mitigation Strategies 4.7 Emerging Technologies in Cybersecurity 4.8 Future Security Challenges and Technological Trends **Suggested Practical Work** • Basic blockchain simulation • Cryptocurrency wallet setup (test network based) • Smart contract deployment and testing (test environment) • Vulnerability identification in sample contracts • IoT security case study analysis • Emerging technology risk assessment report

Reference Books	1. Mastering Bitcoin – Andreas M. Antonopoulos 2. Mastering Ethereum – Andreas M. Antonopoulos & Gavin Wood 3. Blockchain Basics – Daniel Drescher 4. Blockchain Security and Privacy – David Shrier 5. IoT Security – Rohit Gupta 6. Future Crimes – Marc Goodman
Teaching Methodology	Lecture, Demonstration, Case Study, Smart Contract Simulation, IoT Risk Analysis, Research-Based Assignment
Evaluation Method	50% Internal assessment. : - Attendance, Class and home Assignment, Unit test. - Project Assessment, Application development and viva-voce 50% External assessment. : - Theory written examination - Project Assessment, Presentation and viva-voce

[Subject Code-2611000906033001]

Course Code: 604
Course Title: Project

Course Code	604 (Major-16)
Course Title	PROJECT
Credits	4
Course Category	Major Course
Level of Course	400-499 (Advance Level)
Teaching Hours	120 Hours of Applied work(Project)
Minimum Hours/ Semester	120 Hours of Applied work (Project) (Including applied work, E-documentation, viva-voce examination, Project preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	This course is designed to provide students with the opportunity to apply the knowledge and skills they have gained throughout their academic journey in web design, mobile applications, and web technologies. It encourages hands-on learning by developing a real-world, full-scale project through self-exploration of technologies, structured documentation, and effective presentation.
Course Objective	1) Understand and analyze the given project definition and plan development accordingly. 2) Apply learned and self-acquired knowledge of technologies in designing and implementing project solutions. 3) Demonstrate the use of appropriate tools, frameworks, and platforms in project development. 4) Develop a well-structured project document covering all phases of the development life cycle. 5) Present the project effectively using professional communication and presentation tools.
Pre-requisite	Students must have completed foundational and intermediate courses in web design, mobile application development, and web technologies. They should be familiar with programming languages (such as HTML, CSS, JavaScript, Web-technologies/Mobile Technologies, Python, or Java), database concepts, and basic software development practices. Prior experience with mini-projects or assignments involving real-world problem-solving is desirable.
Course Outcomes	**CO1**:Analyze: Students will be able to analyze project requirements, identify suitable tools, and prepare an implementation strategy. **CO2**:Create: Students will develop full-fledged applications using relevant web, mobile, or hybrid technologies. **CO3**:Apply: Students will gain experience in applying the Software Development Life Cycle (SDLC) to real-world problems. **CO4**:Create: Students will prepare and submit a comprehensive project report that meets academic and professional standards.

<table>
<tr><td></td><td>CO5:Evaluate: Students will present their project solutions confidently and clearly to technical and non-technical audiences.</td></tr>
<tr><td>Project Development</td><td>STEP-1: Project Planning and Definition
1.1 Understanding Problem Statement
1.2 Feasibility Study and Requirement Analysis
1.3 Technology Stack Selection (Web, Mobile, Cloud, Database)
1.4 Project Scheduling and Team Role Allocation

STEP-2: Project Design and Architecture
2.1 System Design – High Level and Low Level
2.2 Database Design and ER Diagram
2.3 UI/UX Planning and Wireframing
2.4 Data Flow Diagram and Architecture Diagram

STEP-3: Project Development
3.1 Frontend Development
3.2 Backend Development
3.3 Integration with Database and External APIs
3.4 Testing: Unit Testing, Integration Testing, User Acceptance Testing

STEP-4: Documentation and Deployment
4.1 Preparing Project Documentation: SRS, Design Document, User Manual
4.2 Deployment on Hosting Platforms (like Firebase, Heroku, GitHub Pages, etc.)
4.3 Project Report Writing in Standard Format
4.4 Preparing and Delivering Project Presentation
[Students will submit E-Document for Project report.
One internal guide will be allocated for every ten groups
All groups are required to contact their internal guides once a week to endorse their project progress work.]</td></tr>
<tr><td>Project Evaluation Scheme</td><td><table>
<tr><th>Component</th><th>Marks</th></tr>
<tr><td>Problem Definition and Planning</td><td>10%</td></tr>
<tr><td>Design and Architecture</td><td>15%</td></tr>
<tr><td>Implementation and Functionality</td><td>30%</td></tr>
<tr><td>Testing and Deployment</td><td>15%</td></tr>
<tr><td>Documentation</td><td>10%</td></tr>
<tr><td>Final Presentation & Viva</td><td>20%</td></tr>
<tr><td>Total</td><td>100%</td></tr>
</table></td></tr>
<tr><td>Evaluation Method</td><td>50% Internal assessment.
- Attendance and reporting to internal guides
- Internal project presentation and demonstration, project documentation.
50% External assessment.
- project presentation and demonstration, viva-voce and e-project report.</td></tr>
</table>

[Subject Code-2611000906055001]

Course Code: 605

Course Title: Project and Interview Presentation Soft Skills (AEC-06)

Course Code	605 (Ability Enhancement Course (AEC))
Course Title	Project and Interview Presentation Soft Skills
Credits	2
Course Category	AEC Course
Level of Course	100-199 (Fundamental Level)
Teaching Hours per semester	30 Hours of class-room work
Minimum Hours/ Semester	30 hours of Class-room work (Including class work, interactive sessions, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	The purpose of this course is to equip students from the software, computer, and IT industry with essential project execution, documentation, and presentation skills. It aims to enhance their technical communication, soft skills, and interview preparedness through hands-on project work, seminars, and structured evaluations.
Course Objective	1) To develop students' ability to plan, execute, and manage software/IT projects using industry-standard practices. 2) To enhance technical documentation skills through structured project reports and software documentation. 3) To build confidence in delivering effective oral presentations and technical demonstrations relevant to software and IT domains. 4) To improve soft skills such as teamwork, time management, and problem-solving in a professional IT project environment. 5) To prepare students for technical and HR interviews by practicing mock interviews and resume-building activities.
Pre-requisite	Learners should have a fundamental understanding of programming languages, web or mobile application development, database management, and software development life cycle. Prior exposure to mini-projects or hands-on experience with development tools and technologies used in the IT/software industry will be beneficial.
Course Outcomes	**1) CO1:**(Understand)**:** Explain the essential components of professional project documentation and communication in the software and IT industry. **2) CO2:**(Apply)**:** Demonstrate the ability to present project concepts clearly using structured presentation techniques and visual aids relevant to IT solutions. **3) CO3:**(Analyze)**:** Evaluate the technical and soft skill requirements of various IT job roles and align personal project work and presentation accordingly.

	4) **CO4:**(Create)**:** Develop a mini-project or prototype by integrating appropriate software tools and technologies and document it as per standard industry practices. 5) **CO5:**(Evaluate)**:** Justify design choices, tool selection, and development approach during interviews or viva presentations using logical reasoning and industry-specific language.
Mapping between Course Outcomes(CO) with Program Specific Outcomes(PSO)	

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8
CO1		-			-		-	-
CO2			-	-		-	-	-
CO3		-	-		-	-		-
CO4	-	-		-	-		-	
CO5		-	-		-			

Course Content

Unit 1: Communication and Presentation Skills in the IT Industry

1.1 Fundamentals of Communication
- 1.1.1 Verbal and Non-verbal Communication
- 1.1.2 Barriers in Communication in Technical Teams
- 1.1.3 Listening and Clarity in Technical Discussions

1.2 Presentation Skills for IT Professionals
- 1.2.1 Creating Technical Presentations
- 1.2.2 Using Tools like PowerPoint, Canva, Prezi
- 1.2.3 Speaking with Confidence in Team and Client Meetings

1.3 Email and Technical Writing Etiquette
- 1.3.1 Writing Clear Technical Emails
- 1.3.2 Preparing Professional Reports and Documentation

Unit 2: Project Documentation and Reporting

2.1 Understanding Software Development Life Cycle (SDLC)
- 2.1.1 Role of Documentation at Each Phase
- 2.1.2 Agile Documentation vs Traditional Models

2.2 Technical Project Documentation
- 2.2.1 Problem Statement and Requirements
- 2.2.2 Design Diagrams: UML, ER Diagrams
- 2.2.3 Testing and Deployment Documentation

2.3 Final Report Writing and Formatting
- 2.3.1 Structuring a Complete Project Report
- 2.3.2 IEEE/ACM Style Guidelines and Referencing
- 2.3.3 Common Errors to Avoid in Technical Reports

Unit 3: Interview Readiness and Soft Skills for Developers

3.1 Resume and LinkedIn Profile Building
- 3.1.2 Components of a Tech Resume
- 3.1.3 Tailoring Resumes for Software Roles

3.2 Interviewing Skills for IT Roles
- 3.2.1 Understanding the Interview Process in Software Companies
- 3.2.2 Technical Round vs HR Round Expectations
- 3.2.3 STAR Method for Behavioral Interview Questions

3.3 Mock Interview Sessions

3.3.1 Self-Introduction Practice

3.3.2 Group Feedback and Interview Etiquette

Unit 4: Final Project Presentation and Seminar

4.1 Project Showcase Guidelines
- 4.1.1 Preparing for Project Presentation
- 4.1.2 Demonstrating Code, UI, and Deployment

4.2 Seminar and Peer Review
- 4.2.1 Presentation to Class and Faculty Panel
- 4.2.2 Peer Evaluation Criteria

4.3 Soft Skill Reflection and Final Assessment

	4.3.1 Student Reflections on Soft Skills Gained 4.3.2 Final Grading and Suggestions for Improvement [One topic will be allocated to every students. The student will prepare a seminar and presentation along with a documentation.]
Reference Books	1) Technical Communication: Principles and Practice, Meenakshi Raman & Sangeeta Sharma, Oxford University Press India, ISBN: 9780195695747 2) Soft Skills: Know Yourself and Know the World, Dr. Alex K., S. Chand Publishing, ISBN: 9789352534357 3) Communication Skills for Engineers, Sunita Mishra & C. Muralikrishna, Pearson Education India, ISBN: 9788131733844 4) Business Communication, P.D. Chaturvedi & Mukesh Chaturvedi, Pearson Education India, ISBN: 9788131733585 5) Developing Soft Skills, Gajendra Singh Chauhan, Wiley India, ISBN: 9788126577500 6) The Quick and Easy Way to Effective Speaking, Dale Carnegie, Simon & Schuster, ISBN: 9780743528322 7) Cracking the Coding Interview, Gayle Laakmann McDowell, CareerCup, ISBN: 9780984782857 8) Presentation Skills for Technical Professionals, Naomi Karten, Dorset House Publishing, ISBN: 9780932633585 9) Interviewing: Principles and Practices, Charles Stewart & William Cash Jr., McGraw-Hill Education, ISBN: 9780078036804 10) The Art of Public Speaking, Stephen E. Lucas, McGraw-Hill Education, ISBN: 9780073523910
Teaching Methodology	Class Work, Discussion, Presentation, Self-Study, Seminars and/or Assignments
Evaluation Method	50% Internal assessment. - Attendance, Class and home Assignment, Unit Tests (Seminar). - Internal presentations, documentation, viva-voce and Seminar 50% External assessment. - Presentation, documentation, presentation and Viva-voce.

[Subject code-2611000906066001]

Course Code: 606

Course Title: Internship

Course Code	606
Course Title	Internship
Credits	4
Course Category	Internship
Level of Course	400-499 (Advance Level)
Teaching Hours	120 Hours of internship work
Minimum Hours/ Semester	120 hours of internship work (Including industrial visit, interactive sessions, applied/training work, examination, preparation etc.)
Review / Revision	-
Implementation Year:	A.Y. 2026-2027
Purpose of Course	NEP-2020 emphasizes on Vocationalization of Education. A key aspect of the new UG programme is its utility into a real life situation. All students are expected to do Internships/Apprenticeships/OJT in a firm, industry, or organization. Students will be provided the opportunities for do Internships/Apprenticeships/OJT with local industry, business organizations, health, and allied areas, local governments (such as panchayats, and municipalities), local Police Stations, Parliament or elected representatives, media organizations, artists, crafts persons, and a wide range of organizations so that students may engage with the practical side of their learning, which will improve their employability.
Course Objective	1) To provide students with practical exposure to industry standards and practices. 2) To foster the application of academic knowledge in real-life work scenarios. 3) To enhance students' interpersonal, communication, and problem-solving skills. 4) To help students identify their strengths and areas of interest in professional domains. 5) To inculcate a sense of responsibility, discipline, and work ethics.
Pre-requisite	Students must have completed at least one year of their undergraduate program. They should have basic conceptual knowledge of their core subjects before starting the internship.
Course Outcomes	1) **CO1 (Apply):** Apply programming, development, or analytical skills gained in the classroom to solve real-world computing problems during the internship. 2) **CO2 (Analyze):** Analyze the architecture, workflow, and practices of the host organization to understand the integration of computer systems in business or technical environments. 3) **CO3 (Evaluate):** Evaluate project requirements, software tools, and technologies used during the internship to recommend improvements or alternative approaches. 4) **CO4 (Create):** Create a structured technical report and project documentation summarizing the tasks, challenges, and outcomes of the internship. 5) **CO5 (Present):** Present the project findings and experience effectively using professional communication and presentation skills tailored to the IT/software industry.

Internship Structure and Deliverable by Students:

Duration: 120 Hours
Mode: Offline / Online / Hybrid
Location: Industry, business firms, IT companies, local government offices, health organizations, media, artisans, etc.
Deliverables by Student:

1. Internship Joining Report
2. Weekly Progress Logbook
3. Project or Assignment Work (if applicable)
4. Final Internship Report (with photographs, certificates, etc.)
5. Presentation and Viva Voce

Course Evaluation

Component	Marks/Weightage
Attendance and Participation	20%
Weekly Progress Logbook	20%
Final Internship Report	30%
Presentation & Viva Voce	30%
Total	**100%**

Reference Books

INTERNSHIP REPORT TEMPLATE (to be submitted after internship completion)

Front Page

Title: *Internship Report*
Student Name:
Roll Number:
Program and Semester:
College Name and Department:
Name of Organization/Company:
Internship Duration (From – To):
Internship Guide Name (Industry and Faculty):
Submission Date:

1. Acknowledgment
A short paragraph acknowledging the guidance and support of the organization and faculty mentor.

2. Certificate
Internship Completion Certificate (copy from organization)

3. Declaration
Declaration by the student that the report is original and submitted for academic purposes.

4. Internship Details
Name and Address of Organization
Nature of Business/Services
Department/Team worked in
Name and Designation of Industry Supervisor

5. Objectives of Internship
What you aimed to learn and accomplish.

6. Description of Work Done
Overview of the tasks and responsibilities handled
Description of technologies/tools used
Screenshots, flowcharts, or diagrams (if applicable)

7. Learning Outcomes
Skills developed, software or tools learned, industry exposure gained.

8. Challenges and Solutions
Mention any problems faced and how you solved them.

9. Weekly Summary
Brief of what was done in each week (can be derived from the logbook).

10. Conclusion
Summary of overall experience, learning, and impact on career development.

11. References
Any websites, books, or resources referred to during the internship.

INTERNSHIP LOGBOOK FORMAT (to be maintained weekly)

Week No.	Date (From–To)	Tasks Assigned	Tasks Completed	Tools/Technologies Used

	Week 1	01/06/2025–07/06/2025	Task 1 description	Task 1 completed	e.g., HTML, Python, MySQL		Sig co
	Week 2						
	...						
	Week N						
	Note: The logbook must be signed weekly by the industry/place of internship allocated supervisor and finally verified by the faculty mentor allocated by the institute.						

University Examinations

Course Code	Course	Exam Component	Max. Marks	Duration
601-01 (Minor-5-01)	E-Commerce and Cyber Security	**Theory**	**50**	**2 Hours**
601-02 (Minor-5-02)	Concepts of A.I. and IoT Devices			
601-03 (Minor-5-03)	Computer Graphics			
602-04 (Major-14)	Advanced Security Operations and Threat Hunting	**Theory**	**25**	**1 Hours**
		Project	**25**	**-**
603-04 (Major-15-01)	Blockchain and Emerging Technologies Security	**Theory**	**25**	**1 Hours**
		Project	**25**	**-**
604 (Major-16)	PROJECT	**Project**	**50**	**-**
605 (AEC-06)	Project and Interview Presentation Soft Skills	**Seminar/Presentation**	**50**	**-**
606 (Major)	Internship	**Project report/ presentation/ viva-voce**	**100**	**-**

[University theory exams Course code: 601-01/601-02/601-03, 602, 603-01/603-02and 605 will be scheduled between 5th February to 11th February. Following to the theory exams, students will work on full time Projects and Internship. Project exams will be scheduled between 10th April to 20th April.]