Regulations and Curriculum for

Master of Technology (M. Tech.)
in Cyber Security

(Deemed to be University under Section 3 of UGC Act, 1956)
(Placed under Category 'A' by MHRD, Govt. of India, Accredited with 'A+' Grade by NAAC)
University Enclave, Medical Sciences Complex, Deralakatte,
Mangalore – 575 018, Karnataka INDIA
Tel: +91-824-2204300/01/02/03, Fax: 91-824-2204305
Website: www.nitte.edu.in E-mail: info@nitte.edu.in

REGULATIONS GOVERNING
THE DEGREE OF MASTER OF TECHNOLOGY (M.Tech.)

UNDER OUTCOME BASED EDUCATION (OBE)

AND

CHOICE BASED CREDIT SYSTEM (CBCS) SCHEME

OF

NMAM INSTITUTE OF TECHNOLOGY, NITTE

(Effective from academic year 2022 -23)

VISION

To build a humane society through excellence in the education and healthcare

MISSION

To develop
Nitte (Deemed to be University)
As a centre of excellence imparting quality education,
Generating competent, skilled manpower to face the scientific and social challenges with a high degree of credibility, integrity, ethical standards and social concern

NITTE (Deemed to be University) | NMAM INSTITUTE OF TECHNOLOGY

Off-campus Centre, Nitte (Deemed to be University)

NITTE-574110, Karkala Taluk, Udupi District, Karnataka, India

Vision Statement

Pursuing Excellence, Empowering people, Partnering in Community Development

Mission Statement

To develop N.M.A.M. Institute of Technology, Nitte, as Centre of Excellence by imparting Quality Education to generate Competent, Skilled and Humane Manpower to face emerging Scientific, Technological, Managerial and Social Challenges with Credibility, Integrity, Ethics and Social Concern.

M. Tech. Regulations and Curriculum

Batch

2022 – 2024

With Scheme of Teaching & Examination

REGULATIONS: 2022
for
M. Tech. Programs
(Academic year 2022-23)

COMMON TO ALL
MTech. DEGREE PROGRAMS
CHOICE BASED CREDIT SYSTEM (CBCS)

Key Information

Program Title	Master of Technology, abbreviated as MTech. (Cyber Security)
Short description	Two-year, four semester Choice Based Credit System (CBCS) type of Postgraduate Engineering Degree Program with English as medium of instruction
Program Code	22ENGR140D2
Revision version	2022.02 These regulations may be modified from time to time as mandated by the policies of the University. Revisions are to be recommended by the Board of Studies for **Computer Science Engineering** and approved by the Academic Council.
Effective from	12-09-2022
Approvals	• Approved in the 50th meeting of Academic Council of NITTE (Deemed to be University), held on 30-05-2022 and vide Notification of NITTE (DU), N(DU)/REG/N-MCE/2022-23/76B dated 19-08-2022. • Notification of Nitte (DU), N(DU)/REG/AC/-SA/2022-23/909 dated 24-04-2023.
Program offered at	NMAM Institute of Technology, Nitte Off Campus Centre, Nitte (Deemed to be University)
Grievance and dispute resolution	All disputes arising from this set of regulations shall be addressed to the Board of Management. The decision of the Board of Management is final and binding on all parties concerned. Further, any legal disputes arising out of this set of regulations shall be limited to jurisdiction of Courts of Mangalore only.

Contents

1. INTRODUCTION:

1.1 The general regulations are common to all Degree of Master of Technology Program under Outcome Based Education (OBE) and Choice Based Credit System (CBCS) conducted by Nitte (Deemed to be University), at the NMAM Institute of Technology, Nitte off Campus Centre and shall be called "Nitte (DU) Regulations for M.Tech.- 2022".

1.2 The provisions contained in this set of regulations govern the policies and procedures on the Registration of students, imparting Instructions of course, conducting of the examination and evaluation and certification of students' performance and all amendments there to leading to the said degree program(s)

1.3 This set of Regulations, on approval by the Academic Council and Governing Council, shall supersede all the corresponding earlier sets of regulations of the M.Tech. Degree program (of Nitte (DU)) along with all the amendments thereto, and shall be binding on all students undergoing M.Tech. Degree Program (s) (Choice Based Credit System) conducted at the NMAMIT, Nitte with effect from its date of approval and is applicable for students admitted to 1st year after September 2022. This set of regulations may evolve and get modified or changed through appropriate approvals from the Academic Council / Governing Council from time to time, and shall be binding on all stake holders, (the Students, Faculty, Staff of Departments of NMAMIT, Nitte). The decision of the Academic Council/ Governing Council shall be final and binding.

1.4 In order to guarantee fairness and justice to the parties concerned in view of the periodic evolutionary refinements, any specific issues or matters of concern shall be addressed separately, by the appropriate authorities, as and when found necessary.

1.5 The Academic Council may consider any issues or matters of Concern relating to any or all the academic activities of the NMAMIT courses for appropriate action, irrespective of whether a reference is made here in this set of Regulations or otherwise.

1.6 The course shall be called **Master of Technology** program abbreviated as M.Tech. (Cyber Security) – Choice Based Credit System.

2. DEFINITIONS OF KEYWORDS:

The following are the definitions/ descriptions thathave been followed for the different terms used in the Regulations of M.Tech. Programs:

2.1 Program: Is an educational program in a particular stream/branch of Engineering/branch of specialization leading to award of Degree. It involves events/activities, comprising of lectures/ tutorials/ laboratory work/ field work, outreach activities/ project work/ vocational training/ viva/ seminars/ Internship/ assignments/ presentations/ self-study etc., or a combination of some of these.

2.2 Branch: Means Specialization or discipline of M. Tech Degree Program, like Electrical Vehicle Technology, Structural Engineering, Machine Design, etc.

2.3 Semester: Refers to one of the two sessions of an academic year (vide: serial number 4), each session being of sixteen weeks duration (with working days greater than or equal to 90). The odd semester may be scheduled from August/September and even semester from February/March of the year.

2.4 Academic Year: Refers to the sessions of two consecutive semesters (odd followed by an even) including periods of vacation.

2.5 Course: Refers to usually referred to as 'subjects' and is a component of a program. All Courses need not carry the same credit weightage. The Courses should define learning objectives and learning outcomes. A Course may be designed to comprise lectures/ tutorials/ laboratory work/ field work/ outreach activities/ project work/ vocational training/ viva/ seminars/ term papers/ assignments/ presentations/ self- study etc. or a combination of some of these.

2.6 Credit: Refers to a unit by which the Course work is measured. It determines the number of hours of instructions required per week. One credit is equivalent to one hour of lecture or two hours of laboratory/ practical Courses/ tutorials/ fieldwork per week etc.

2.7 Audit Courses: Means Knowledge/ Skill enhancing Courses without the benefit of credit for a Course.

2.8 Choice Based Credit System (CBCS): Refers to customizing the Course work, through Core, Elective and soft skill Courses, to provide necessary support for the students to achieve their goals.

2.9 Course Registration: Refers to formal registration for the Courses of a semester (Credits) by every student under the supervision of a Faculty Advisor (also called Mentor, Counsellor etc.,) in each Semester for the Institution to maintain proper record.

2.10 Course Evaluation: Means Continuous Internal Evaluation (CIE) and Semester End Examinations (SEE) to constitute the major evaluations prescribed for each Course. CIE and SEE to carry 50 % and 50 % respectively, to enable each Course to be evaluated for 100 marks, irrespective of its Credits.

2.11 Continuous Internal Evaluation (CIE): Refers to evaluation of students' achievement in the learning process. CIE shall be by the Course Instructor and includes tests, homework, problem solving, group discussion, quiz, mini-project and seminar throughout the Semester, with weightage for the different components being fixed at the University level.

2.12 Semester End Examinations (SEE): Refers to examination conducted at the University level covering the entire Course Syllabus. For this purpose, Syllabi to be modularized and SEE questions to be set from each module, with a choice confined to the concerned module only. SEE is also termed as university examination.

2.13 Make Up Examination: Refers to examination conducted for the candidates who has a CIE>=35 marks and may have missed to attend the SEE covering the entire course syllabus. The standard of Make Up Examination is same as that of the SEE.

2.14 Supplementary Examination: Refers to the examination conducted to assist slow learners and/or failed students through make up courses for a duration of 8 weeks. This comprises of both the CIE & SEE and will be conducted after the completion of First year M.Tech. even semester.

2.15 Credit Based System (CBS): Refers to quantification of Course work, after a student completes teaching – learning process, followed by passing in both CIE and SEE. Under CBS, the requirement for awarding Degree is prescribed in terms of total number of credits to be earned by the students.

2.16 Credit Representation: Refers to Credit Values for different academic activities considered, as per the Table.1. Credits for seminar, project phases, project viva–voce and internship shall be as specified in the Scheme of Teaching and Examination.

Table 1: Credit Values

Theory/Lectures (L) (hours/week/Semester)	Tutorials (T) (hours/week/ Semester)	Laboratory /Practical (P) (hours/week/ Semester)	Credits (L: T:P)	Total Credits
4	0	0	4:0:0	4
3	0	0	3:0:0	3
2	2	0	2:1:0	3
2	0	2	2:0:1	3
2	2	2	2:1:1	4
0	0	2	0:0:1	1

NOTE: Activities like, practical training, study tour and participation in Guest lectures not to carry any credits.

2.17 Letter Grade: It is an index of the performance of students in a said Course. Grades are denoted by letters O, A+, A, B+, B, C and F.

2.18 Grading: Grade refers to qualitative measure of achievement of a student in each Course, based on the percentage of marks secured in (CIE+SEE). Grading is done by Absolute Grading. The rubric attached to letter grades are as follows:

Letter Grade	O	A+	A	B+	B	C	F
Academic Level	Outstanding	Excellent	Very Good	Good	Above Average	Average	Fail

2.19 Grade Point (GP): Refers to a numerical weightage allotted to each letter grade on a 10-point scale as under.

Letter Grade and corresponding Grade Points on a typical 10 – Point scale							
Letter Grade	O	A+	A	B+	B	C	F
Grade Point	10	09	08	07	06	05	00

2.20 Passing Standards: Refers to passing a Course only when getting GP greater than orequal to 05 (as per serial number 2.20).

2.21 Credit Point: Is the product of grade point (GP) and number of credits for a Coursei.e., Credit points CrP = GP × Credits for the Course.

2.22 Semester Grade Point Average (SGPA): Refers to a measure of academic performance of student/s in a semester. It is the ratio of total credit points secured by astudent in various Courses of a semester and the total Course credits taken during thatsemester.

2.23 Cumulative Grade Point Average (CGPA): Is a measure of overall cumulative performance of a student over all semesters. The CGPA is the ratio of total credit pointsearned by a student in various Courses in all semesters and the sum of the total creditsof all Courses in all the semesters. It is expressed up to two decimal places.

2.24 Grade Card: Refers to a certificate showing the grades earned by a student. A grade card shall be issued to all the registered students after every semester. The grade card will display the program details (Course code, title, number of credits, grades secured) along with SGPA of that semester and CGPA earned till that semester.

2.25 University: Nitte (Deemed to be University), Mangalore. NMAM Institute of Technology is an off-campus centre of Nitte (DU) and located at Nitte.

3. CLAUSE

CLAUSE	PARTICULARS
22NMT1.0	**DURATION AND CREDITS OF THE PROGRAM OF STUDY** There shall be one category of program: Full-time Program (FT) **Full-time Program:** The Program shall extend over a period of four semesters (2 years). **First Semester:** i) 16 weeks – Class Work according to the scheme. ii) 4 weeks – Revision holidays and examinations iii) 2 weeks – Vacation **Second Semester:** i) 16 weeks – Class Work according to the scheme ii) 4 weeks – Revision holidays and examinations. **Summer Semester/Vacation** i) 4 weeks — Class work, Examination & Display of Grades **Third Semester: 20 weeks** i) 8 weeks — Industrial Training/Mini Project ii) 12 weeks — Project Part-I— Industrial Training/Mini Project evaluation, Seminar on SpecialTopic Evaluation & Project Part-I Evaluation **Fourth Semester: 24 weeks** i) 22 weeks — Project Part-II ii) 2 weeks – Submission, viva -voce **Prescribed Number of Credits for the Program: 80** iii) The number of credits to be completed for the award of Degree shall be 80.

22NMT1.1

M.Tech Degree Programs are offered in the following specialization and the respective program hosting departments are listed below:

Program	**Department**
i) Computer Science & Engineering	Computer Science & Engineering
ii) Constructional Technology	Civil Engineering
iii) Structural Engineering	Civil Engineering
iv) VLSI Design & Embedded Systems	Electronics and Communication Engineering
v) Machine Design	Mechanical Engineering
vi) Energy Systems Engineering	Mechanical Engineering
vii) Cyber Security	Computer Science Engineering
viii) Electric Vehicle Technology	Electrical and Electronics Engineering

The provisions of these Regulations shall be applicable to any new specialization that may be introduced from time to time and appended to the above list.

22NMT1.2

Maximum Duration for Program Completion:

A full-time candidate shall be allowed a maximum duration of 4 years from the I semester of admission to become eligible for the award of master's degree, failing which he/she may discontinue of register once again as a fresh candidate to I semester of the program.

22NMT2.0

ELIGIBILITY FOR ADMISSION

(As per the Government orders issued from time to time):

Admission to I year/ I semester Master of Technology Program shall be open to all the candidates who have passed B.E./ B. Tech. Examinations (in relevant field) or any other recognized University/ Institution. AMIE in respective branches shall be equivalent to B.E./ B. Tech. Programs for admission to M.Tech. The decision of the equivalence committee shall be the final in establishing the eligibility of candidates for a particular Program.

For the foreign Degrees, Equivalence certificate from the Association of Indian Universities shall be a must.

22NMT2.1	Admission to M.Tech. Program shall be open to the candidates who have passed the prescribed qualifying examination with not less than 50% of the marks in the aggregate of all the years of the Degree examination. Rounding off percentage secured in qualifying examination is not permissible.
22NMT2.2	**For admissions under GATE/ NUCAT qualification** The candidates should be GATE qualified or should have appeared for the NUCAT Entrance Examination conducted by Nitte (Deemed to be University) [Nitte (DU)]
22NMT2.3	**For admissions under Sponsored Quota:** The candidates should be GATE qualified or should have appeared for the NUCAT Entrance Examination conducted by Nitte (DU)
22NMT2.4	The candidates, who are qualified in the GATE Examination for the appropriate branch of engineering, shall be given priority. They are exempted from taking NUCAT Entrance Examination. In case a GATE qualified Candidate appears for entrance examination and become qualified to claim a seat under entrance examination quota, he/she will be considered in the order of merit along with other candidates appeared for the entrance examination.
22NMT2.5	If sufficient number of GATE qualified candidates are not available, the remaining vacant seats shall be filled from amongst the candidates appeared for NUCAT Entrance Examination in the order of merit.
22NMT2.6	Engineering graduates other than the Karnataka candidates shall get their Eligibility verified from Nitte (DU) to seek admission to M.Tech. Program at NMAMIT, Nitte
22NMT2.7	**Admission to vacant seats:** Seats remaining vacant (unfilled), after the completion of admission process through GATE/NUCAT Entrance Exam, the remaining seats shall be filled by Candidates based on merit in the entrance test conducted at the Institution level. An admission Committee, consisting of the Principal, Head of the concerned Department and the subject experts, shall oversee admissions.
22NMT3.0	**REGISTRATION:** Every student after consulting his **Faculty-Advisor** in parent department is required to register for the **approved courses** with the **Departmental Post**

Graduate Committee (DPGC) of Parent Department at the commencement of each Semester on the days fixed for such registration and notified in the academic calendar.

22NMT3.1

Lower and Upper Limits for Course Credits Registered in a Semester.

Course Credit Assignment:

All courses comprise of specific Lecture/ Tutorial/ Practical (L-T-P) schedule. The course credits are fixed based on the following norms.

Lecture/Tutorials/ Practical:

(i) a 1-hour Lecture per week is assigned 1.0 Credit.

(ii) a 2-hour Tutorial session per week is assigned 1.0 Credit.

(iii) a 2-hour Lab. session per week is assigned 1.0 credits

For example, a theory course with L-T-P schedule of 3-2-0 hours will be assigned 4.0 credits.

A laboratory practical course with L-T-P schedule of 0-0-2 hours will be assigned 1.0 credit.

Calculation of Contact Hours / Week – A Typical Example

Typical Academic Load (I & II Semester)				
No. of Courses	**LTP**	**Credits Per course**	**Total Credits**	**Contact Hours per Week**
2 Lecture Courses	4-0-0	04	08	08
2 Lab Courses	0-0-2	01	02	04
1 Research based Course	0-0-4	02	02	04
3 Elective Courses	3-0-0	03	09	09
1 Audit Course	2-0-0	0	0	02
Total: 9 Courses			21	27

A student must register, as advised by Faculty Advisor, between a minimum of 16 credits and up to a Maximum of 28 credits. However, the minimum/ maximum Credit limit can be relaxed by the Dean (Academic) on the recommendations of the DPGC, only under extremely exceptional circumstances.

22NMT3.2	**Mandatory Pre-Registration for higher semester:** In order to facilitate proper planning of the academic activities of the Semester, it is necessary for the students to declare their intention to register for courses of higher semesters (2nd and above) at least two weeks before the end of the current semester choosing the courses offered by each department in the next higher semester which is displayed on the Departmental Notice Board at least 4 weeks prior to the last working day of the semester. Students who fail to register on or before the specified date will have to pay a late fee. Registration in absentia is allowed only in exceptional cases with the permission of the Dean (Academic). Registration to a higher semester is allowed only if the student fulfills the following conditions- i) Satisfied all the academic requirements to continue with the program of studies without termination. ii) Cleared all institute, hostel and library dues and fines, if any, of the previous semester. iii) Paid all required advance payments of the Institute and the hostel for the current semester. Has not been debarred from registering on any specific grounds by the Institute.
22NMT3.3	**Course Pre-Requisites:** In order for a student to register for some course(s), it may be required either to have completed satisfactorily or to have prior earned credits in some specified course(s). In such instances, the DPGC shall specify clearly, any such course pre-requisites, as part of the curriculum.
22NMT3.4	Students who do not register before the deadline day of registration may be permitted LATE Registration up to the notified day in academic calendar on payment of late fee.
22NMT3.5	REGISTRATION in ABSENTIA will be allowed only in exceptional cases on the recommendation of DPGC through the authorized representative of the student.
22NMT3.6	Medium of Instruction/Evaluation/etc. shall be English.

22NMT4.0	**COURSES:** The curriculum of the Program shall be any combination of following type of courses: i) **Professional Core Courses (PCC)** - relevant to the chosen specialization/ branch [May be split into Hard (no choice) and Soft (with choice), if required]. The core course is to be compulsorily studied by a student and is mandatory to complete the requirements of a program in a said discipline of study. ii) **Professional Electives Courses (PEC)** - relevant to the chosen specialization/ branch: these are the courses, which can be chosen from the pool of papers. It shall be supportive to the discipline/ providing extended scope/enabling an exposure to some other discipline / domain/ nurturing student skills. iii) **Research Experience** Through Practice-I and Research Experience Through Practice-II **iv) Project Work** **v) Seminar** **vi) Audit Courses (AC):** a) The Audit course can be any credit course offered by the program to which the candidate is admitted (other than the courses considered for completing the prescribed program credits) or other programs offered in the institution, where the student is studying. b) The students are required to register for one audit course during I and II semesters. Students who have registered to audit the courses, considered on par with students registered to the same course for credit, must satisfy attendance and CIE requirements. However, they need not have to appear for SEE. c) Registration for any audit course shall be completed at the beginning of I and II semesters. The Department should intimate the Controller of Examination about the registration at the beginning of the semester and obtain a formal approval for inclusion of the audit course/s in the Grade card issued to the students

<table>
<tr><td></td><td>vii) Internship/ Mini Project: Preferably at an industry/ R&D organization/IT company/ Government organization of significant repute or at the Research Centre of parent Institution for a specified period mentioned in Scheme of Teaching and Examination.</td></tr>
<tr><td>22NMT4.1</td><td>Program Structure:
The number of credits to be registered in a semester is between 16 and 28
Minimum Credit Requirement for the M.Tech. Degree is 80.
The total course package for an M.Tech. Degree Program will typically consist of the following components.
<table>
<tr><th>Course type</th><th>Range %</th><th>Suggested Credits</th></tr>
<tr><td>i) Program Core Courses</td><td>20 - 25</td><td>20</td></tr>
<tr><td>ii) Program Elective Courses</td><td>18 - 20</td><td>15</td></tr>
<tr><td>iii) Elective Courses (MOOCS)</td><td>4</td><td>03</td></tr>
<tr><td>iv) Industrial Internship/Research Internship/Mini Project</td><td>10</td><td>08</td></tr>
<tr><td>v) Project</td><td>35</td><td>28</td></tr>
<tr><td>vi) Seminar</td><td>2.5</td><td>02</td></tr>
<tr><td>vii) Research Experience Through Practice</td><td>5</td><td>04</td></tr>
<tr><td>viii)Audit courses (two courses)</td><td>-</td><td>-</td></tr>
<tr><td>Total credits</td><td></td><td>80</td></tr>
</table>
The Department Post Graduate Committee (DPGC) will discuss and recommend the exact credits offered for the program for the above components, the semester-wise distribution among them, as well as the syllabi of all postgraduate courses offered by the department from time to time before sending the same to the Board of Studies (BOS).
The BOS will consider the proposals from the departments and make recommendations to the Academic Council for consideration and approval.
Mandatory Learning Courses:
These are courses that must be completed by the student at appropriate time as suggested by the Faculty Adviser or the DPGC. Courses that come under the category are as following:</td></tr>
</table>

Industrial Training:

This is a 08-credit course. A full-time student will complete the Industrial Training (or a Mini Project) at appropriate time stipulated by DPGC and register for it in the following Semester and shall also submit a bound copy of training report certified by the authority of Training Organization. The duration and the details, including the assessment scheme, shall be decided by the faculty advisor, with approval from DPGC.

Seminar:

This also carries 2-credits to be completed at appropriate time stipulated by DPGC. The student will make presentations on topics of academic interest, as suggested by DPGC.

Research Experience through Practice-I and Research Experience through Practice-II:

- Research Experience through Practice-I and II are 2-credit courses in the first and second semesters respectively.
- The student will work under a faculty supervisor approved by the DPGC and submits a research proposal at the end of the first semester which is evaluated jointly by the faculty supervisor and a co-examiner.
- Students shall be offered inputs like how to conduct a literature survey, how to identify a research problem, how to write a research paper, research report, research proposal, and systematic way of conducting research etc.
- Department specific/PG Program specific skill sets required for carrying out a research work may be offered to the students like software tools for system/device simulation and analysis, software/ hardware tools for signal acquisition, data processing, control simulation, Testing/measuring equipment used in research and Testing/measuring procedure.
- At the end of Research Experience through Practice-I in the first semester, M. Tech. students should be able to identify a research problem, with clear objectives and methodologies backed by extensive literature review.
- Two internal examiners will evaluate the Research Experience through Practice-I out of which one will be the guide and the other examiner will a faculty member who is having expertise in the research area of the student

	being evaluated. The research proposal report and the research proposal presentation are evaluated for 100 marks in the first semester. • The student will work on the proposed research in the second semester and submit a research paper at the end of the second semester which is evaluated jointly by the faculty supervisor and a co-examiner. • In the second semester, the students are expected to carry out Mathematical modelling / Design calculations / computer simulations / Preliminary experimentation / testing of the research problems identified during Research Experience through Practice-I carried out in the first semester. At the end of the second semester, students are expected to write a full research paper based on the Mathematical modelling/ Design calculations/computer simulations/Preliminary experimentation/testing carried out during second semester. The research paper submitted by the student and the presentation of the research work carried out is evaluated for 100 marks in the second semester.
22NMT5.0	**INTERNSHIP/MINI PROJECT:** The student shall undergo Internship/Mini Project as per the Scheme of Teaching and Examination. 1. The internship can be carried out in any industry/R&D Organization/Research Institute/Institute of national repute/R&D Centre of Parent Institute. 2. The Department/college shall nominate a faculty to facilitate, guide and supervise students under internship. 3. The students shall report the progress of the internship/Mini Project to the internal guide in regular intervals and seek his/her advice. 4. The Internship shall be completed during the period specified in Scheme of Teaching and Examination. 5. After completion of Internship/mini project, students shall submit a report to the Head of the Department with the approval of both internal and external guides and with the approval of internal guide if the Internship/Mini-Project is carried out in the Institute.

	6. The Internship/Mini Project will be evaluated jointly by two internal examiners appointed by the Head of the Department/Controller of Examination. 7. The Internship/Mini Project report and the presentation by the student will be evaluated for 50 marks each immediately after completion of the Internship/Mini Project. The students are permitted to carry out the internship anywhere in India or Abroad. The Institution will not provide any kind of Financial Assistance to any student for Internship/Mini Project and for the conduct of Viva-Voce on internship.
22NMT5.1	**Failing to undergo Internship/Mini Project:** Securing a pass grade in Internship/Mini Project is mandatory as a partial requirement for the award of Degree. Internship/Mini Project Securing a pass grade in Internship/Mini Project is mandatory. If any student fails to undergo/complete the Internship/ Mini Project, he/she shall be considered as fail in that Course.
22NMT6.0	**SEMINAR:** Securing a pass grade in Seminar is mandatory as a partial requirement for the award of Degree. i) Each candidate shall deliver seminar as per the Scheme of Teaching and Examination on the topics chosen from the relevant fields for about 30 minutes. The Head of the Department shall make arrangements for conducting seminars through concerned faculty members of the department. The Panel of Examiners constituted for the purpose by the Head of the Department shall award the CIE marks for the seminar.
22NMT7.0	**PROJECT WORK:** Securing a pass grade in Project Work is mandatory as a partial requirement for the award of Degree. Project work shall be on individual basis. **Project Part-I and Part-II:** **Project Part-I: (In third Semester)** The duration of the Project Part-I is of 12 weeks as notified in the academic

calendar. The evaluation of the Project Part-I will be done during the end of third semester.

Each department will prepare the Panel of Examiners in advance and also prepare the Project Part-I evaluation schedule indicating the names of the students, their USN, Title of the Project, Name of the Examiners, and time and Venue of the evaluation which will be submitted to the Controller of Examination Office in advance.

Project Part-I evaluation will be done by two internal Examiners, one of them will be the Guide and other is preferably one of the experts in the area of PG Project being evaluated.

The mark distribution of Project Phase-I evaluation is: 100 marks for report and 100 marks for presentation jointly awarded by the both the examiners.

Project Part-II: (In the fourth Semester)

The total duration of Project Part-II is of 22 weeks as notified in the academic calendar. There will be two Continuous Internal Evaluation of Project Part-II in fourth semester followed by Semester End Evaluation of the Project Phase- II, namely, Project Progress Evaluation-I (PPE-I), Project Progress Evaluation

-II(PPE-II) and SEE.

The same Panel of Examiners which was formed during Project Part-I evaluation is to be continued for the Project Progress Evaluation in the fourth semester.

PPE-I and PPE-II will be scheduled as per the academic calendar and will be evaluated for 100 marks each (50 marks for report and 50 marks for presentation jointly conducted by the two internal examiners).

Each department will prepare the Panel of Examiners in advance and also prepare the Project Part-II Project Progress Evaluation Schedule indicating the names of the students, their USN, Title of the Project, Name of the Examiners, and time and Venue of the evaluation as per the format which will be submitted to the Controller of Examination Office in advance.

For the Off-Campus projects, the Internal Guide should visit the organization in which the M.Tech Student is carrying out his Project at least once during the project term.

	The candidate shall submit a soft copy of the dissertation work to the Institute. The soft copy of the dissertation should contain the entire Dissertation in monolithic form as a PDF file (not separate chapters). The Guide, after checking the report for completeness shall check the report for Plagiarism content. The allowable plagiarism index is less than or equal to 25%. If the check indicates a plagiarism index greater than 25%, the guide should advice the student to resubmit the dissertation after modifying the report. The report has to be once again checked for the plagiarism content and the signed hard copy of the Plagiarism Report along with the two hard copies of the dissertation is to be submitted to the Head of the Institution through the Head of the Department. The dissertation will be evaluated by two examiners, one of the examiners shall be the Guide of the candidate and the other examiner shall be an external expert in the area of the dissertation being evaluated. The guide shall submit panel of two approved external examiners to the office of the Controller of Examination through the head of the Department. The Controller of Examination will randomly select one of the external examiners and invites him/her formally for the evaluation of the dissertation and Viva-Voce examination giving sufficient time for the external examiner for reading the dissertation.
22NMT7.1	The dissertation will be evaluated by two examiners, one of the examiners shall be the guide of the candidate and the other examiner shall be preferably an external expert in the area of the dissertation being evaluated. The evaluation of the dissertation shall be made independently by each examiner.
22NMT7.2	Examiners shall evaluate the dissertation normally within a period of not more than two weeks from the date of receipt of dissertation through email.
22NMT7.3	The examiners shall independently submit the marks for the dissertation during the viva-voce examination date
22NMT7.4	Sum of the marks awarded by the two examiners shall be the final evaluation marks for the Dissertation.

22NMT7.5	(a) Viva-voce examination of the candidate shall be conducted, if the dissertation work and the reports are accepted by the external examiner. (b) If the external examiner finds that the dissertation work is not up to the expected standard and the minimum passing marks cannot be awarded, the dissertation shall not be accepted for SEE. (c) If the dissertation is rejected during the Project Part II, then the Second Examiner (external) will be appointed by the COE against whom the candidate has to re-present the same dissertation. The decision of the Second Examiner (external) will be final. If the second examiner (external) accepts the dissertation, then the viva-voce examination of the candidate shall be conducted as per the norms. If the second examiner (external) rejects the dissertation, then the student has to take an extension for a minimum period of 3 months and re-work on the project. After the completion of the extension period, viva-voce examination of the candidate shall be conducted as per the norms, if the dissertation work is accepted by the external examiner.
22NMT7.6	The candidate, whose dissertation is rejected, can rework on the same topic or choose another topic of dissertation under the same Guide or new Guide if necessary. In such an event, the report shall be submitted within four years from the date of admission to the Program.
22NMT7.7	Viva-voce examination of the candidate shall be conducted jointly by the external examiner and internal examiner/ guide at a mutually convenient date.
22NMT7.8	The relative weightages for the evaluation of dissertation and the performance at the viva-voce shall be as per the scheme of teaching and examination.
22NMT7.9	The marks awarded by both the Examiners at the viva-voce Examination shall be sent jointly to the office of Controller of Examination immediately after the examination.
22NMT7.10	Examination fee as fixed from time to time by the Institute for evaluation of dissertation report and conduct of viva-voce shall be remitted to the Institute as per the instructions of Dean-Academics, from time to time.
22NMT7.11	The candidates who fail to submit the dissertation work within the stipulated time have to apply for the extension of the Project duration through the Guide and the head of the department to the Office of the Controller of Examination.

	Such candidate is not eligible to be considered for the award of rank.
22NMT8.0	**ATTENDANCE REQUIREMENT:** 1. Each semester is considered as a unit and the candidate has to put in a minimum attendance of 85% in each subject with a provision of condoning 10% of the attendance by Principal for reasons such as medical grounds, participation in University level sports, cultural activities, seminars, workshops and paper presentation etc. 2. The basis for the calculation of the attendance shall be the period of term prescribed by the institution in its calendar of events. For the first semester students, the same is reckoned from the date of admission to the course. 3. The students shall be informed about their attendance position in the first week of every month by the College so that the students shall be cautioned to make up the shortage. 4. The head of the department shall notify regularly, the list of such candidates who fall short of attendance. The list of the candidates falling short of attendance shall be sent to the Principal with a copy to Controller of Examinations. 5. A candidate having shortage of attendance (<75%) in any course(s) registered shall not be allowed to appear for SEE of such course(s). Such students will be awarded 'N' grade in these courses. 6. He/she shall have to repeat those course(s) with 'N' grade and shall re-register for the same course(s) core or elective, as the case may be when the particular course is offered next either in a main (odd/even) or summer semester. **7.** If a candidate, for any reason, discontinues the course in the middle he/she may be permitted to register to continue the course along with subsequent batch, subject to the condition that he/she shall complete the class work, lab work and seminar including the submission of dissertation within maximum stipulated period. Such candidate is not eligible to be considered for the award of rank.

22NMT9.0	**ADD/ DROP/ AUDIT OPTIONS:** 1. ADD-option: A student has the option to ADD courses for registration till the date specified for late registration. 2. DROP-option: A student has the option to DROP courses from registration until one week after the mid-semester examination. AUDIT-option: A student can register for auditing a course, or a course can even be converted from credit to audit or from audit to credit, with the consent of faculty advisor and course instructor until one week after the mid-semester exam. However, CORE courses shall not be made available for audit. It is not mandatory for the student to go through the regular process of evaluation in an audit course. However, the student has to keep the minimum attendance requirement, as stipulated by the corresponding DPGC for getting the 'U' grade awarded in a course, failing which that course will not be listed in the Grade Card.
22NMT10.0	**ABSENCE DURING THE SEMESTER:** **Leave of Absence** (a) If the period of leave is more than two days and less than three weeks, prior application for leave shall have to be submitted to the Head of the Department concerned, with the recommendation of the Faculty-Advisor stating fully the reasons for the leave request along with supporting documents. It will be the responsibility of the student to intimate the course instructors, Head of the Department and also Chief Warden of the hostel, regarding his absence before availing leave.
22NMT10.1	**Absence during Mid-Semester Examinations:** A student who has been absent from a Mid-Semester Examination (MSE) due to illness and other contingencies may give a request for additional MSE within two working days of such absence to the office of the respective Head of the Department (HOD) with necessary supporting documents and certification from authorized personnel. The HOD may consider such requests depending on the merits of the case, may permit the additional Mid-Semester Examination for the concerned student.

22NMT10.2	**Absence during Semester End Examination:** In case of absence for a Semester End Examination, on medical grounds or other special circumstances the student can apply for 'I' grade in that course with necessary supporting documents and certifications by authorized personnel to the Controller of Examination through Chairman of The Department. The Controller of Examination may consider the request depending on the merits of the case and permit the make-up Semester End Examination for the concerned student. The student may subsequently complete all course requirements within the date stipulated by DPGC (which may be extended till first week of next semester under special circumstances) and 'I' grade will then be converted to an appropriate letter grade. If such an application for the 'I' grade is not made by the student, then a letter grade will be awarded based on his in-semester performance.
22NMT11.0	**WITHDRAWAL FROM THE PROGRAM:** **Temporary Withdrawal:** A student who has been admitted to a Post Graduate Degree program of the College may be permitted to withdraw temporarily, for a period of one semester or more on the grounds of prolonged illness or grave calamity in the family etc. The student should abide by the applicable rules and regulations of the college/University at the time of Temporary Withdrawal.
22NMT11.1	**Permanent Withdrawal:** Any student who withdraws admission before the closing date of admission for the Academic Session is eligible for the refund of the deposits only. Fees once paid will not be refunded on any account. Once the admission for the year is closed, the following conditions govern withdrawal of admissions: a) A student who wants to leave the College for good, will be permitted to do so (and can take Transfer Certificate from the College, if needed), only after remitting the Tuition fees as applicable for all the remaining semesters and clearing all other dues, if any. b) Those students who have received any scholarship, stipend or other forms of assistance from the College shall repay all such amounts in addition to those mentioned in (a) above.

	The decision of the Principal of the Institute regarding withdrawal of a student is final and binding.
22NMT12.0	**EVALUATION SYSTEM:** Continuous Internal Evaluation (CIE) and Semester End Evaluation (SEE)
22NMT12.1	For all the theory and laboratory courses, the CIE marks shall be 50. For Research Experience through Practice-I, Research Experience through Practice-II, seminar, Industrial Training/Mini Project, the CIE marks shall be 100. For Project Phase-I, the CIE Marks shall be 200 For Project Phase-II, the CIE Marks shall be 200 and for SEE 200
22NMT12.2	CIE Marks for courses shall be based on a) Tests MSE-I and MSE-II (for 30 Marks): MSE in a theory course, for 30 marks, shall be based on two tests covering the entire syllabus. Assignments, Quizzes, Simulations, Experimentations, Mini project, oral examinations, field work etc., (for 20 Marks) conducted in respective courses.
22NMT12.3	a) An additional MSE may be conducted for those students absent for valid reasons/ with prior permission. b) For those students who could not score minimum required CIE marks (25 marks), an additional MSE may be conducted, however the maximum CIE marks shall be restricted to 25 out of 50.
22NMT12.4	The candidates shall write the Tests in Blue Book/s. The Blue book/s and other documents relating to award of CIE marks shall be preserved by the Head of the Department for at least six months after the announcement of University results and made available for verification at the directions of the Controller of Examination.
22NMT12.5	Every page of the CIE marks list shall bear the signatures of the concerned Teacher and Head of the Department.
22NMT12.6	The CIE marks list shall be displayed on the Notice Board and corrections, if any, shall be incorporated before submitting to the office of the Controller of Examination (COE).
22NMT12.7	The CIE marks shall be sent to the office of the COE well in advance before the commencement of Semester End Examinations. No corrections of the CIE

	marks shall be entertained after the submission of marks list to the Office of the COE.
22NMT12.8	Candidates obtaining less than 50% of the CIE marks in any course (Theory /Laboratory/ Seminar/ Internship/ Project) shall not be eligible to appear for the Semester end examination in that course/s. In such cases, the Head of the Department shall arrange for the improvement of CIE marks in the course/ Laboratory when offered in the subsequent semester subject to the maximum duration allowed for completion of a M.Tech. program.
22NMT12.9	**Semester End Evaluation:** There shall be a Semester End Examination at the end of each semester.
22NMT12.10	There shall be double valuation of theory papers. The theory Answer booklets shall be valued independently by two examiners appointed by the Controller of Examination.
22NMT12.11	If the difference between the marks awarded by the two examiners is not more than 15 per cent of the maximum marks, the marks awarded to the candidate shall be the average of two evaluations.
22NMT12.12	If the difference between the marks awarded by the two examiners is more than 15 per cent of the maximum marks, the answer booklet shall be evaluated by a third Examiner appointed by the Controller of Examination. The average of the marks of nearest two valuations shall be considered as the marks secured by the candidate. In case, if one of the three marks falls exactly midway between the other two, then the highest two marks shall be taken for averaging.
22NMT12.13	**Summer Semester:** Summer semester is primarily to assist weak and/or students having N/F grade in courses, for a duration of 4 weeks after the completion of regular even SEE. The institute may also offer Add-on/ Audit Courses during this semester.
22NMT12.14	Each candidate shall obtain not less than 50% of the maximum marks (25 marks) prescribed for the CIE of each subject, including seminars. CIE Marks shall be based on assignments, tests, oral examinations and seminar (minimum of two are compulsory) conducted in respective subjects. The candidates obtaining less than 50% of the CIE marks in any subject shall not be eligible to appear for the SEE in that subject(s). Only in such cases, the Controller of Examination may arrange for reregistering the subject(s) in

	subsequent semester or may refer to DPGC for necessary remedial measures. The candidates shall write the Internal Assessment Test in Blue Books, and this shall be maintained by the Head of the Department for at least six months after the announcement of result and is available for verification. The CIE marks sheet shall bear the signature of the concerned Teacher and the Chairman of the Department. The CIE marks list shall be displayed on the Notice Board and corrections, if any, shall be incorporated before sending to the Controller of Examinations.
22NMT12.15	The Academic Performance Evaluation of a student shall be according to a Letter Grading System, based on the Class Performance Distribution. The Letter grades O, A+, A, B+, B, C and F indicate the level of academic achievement, assessed on a decimal (0-10) scale. The Letter grade awarded to a student in a course, for which he has registered shall be based on his performance in quizzes, tutorials, assignments etc., as applicable, in addition to two mid-semester examination and one semester end examination. The distribution of weightage among these components may be as follows: Semester End Examination (SEE) 50% Continuous Internal Evaluation (CIE) (i) Quizzes, Tutorials, Assignments etc., 20% (ii) Mid-semester Examination: 30% Any variation, other than the above distribution, requires the approval of the pertinent DPGC and Academic Council. The letter grade awarded to a student in a 0-0-P (Practical) course, is based on an appropriate continuous evaluation scheme that the course instructor shall evolve, with the approval of the pertinent DPGC. The course Instructor shall announce in the class, and/or display in the display boards or at the website, the details of the Evaluation Scheme, including the distribution of the weightage for each of the components, and method of conversion from the raw scores to the letter-grades; within the first week of the semester in which the course is offered, so that there are no ambiguities in communicating the same to all the students concerned.

22NMT12.16	**The Transitional Grades** 'I', 'W' and 'X' would be awarded in the following cases. These would be converted into one or the other of the letter grades (O-F) after the student completes the course requirements. **Grade "I":** To a student having attendance ≥85% and CIE ≥ 70%, in a course, but remained absent from SEE for valid & convincing reasons acceptable to the College, like: i. Illness or accident, which disabled him/her from attending SEE. ii. A calamity in the family at the time of SEE, which required the student to be away from the College. iii. However, the committee chaired by the Principal is authorized to relax the requirement of CIE ≥ 70% if the student is hospitalized or advised long term rest after discharge from the hospital by the Doctor. iv. Students who remain absent for Semester End Examinations due to valid reasons and those who are absent due to health reasons are required to submit the necessary documents along with their request to the Controller of Examinations to write Make up Examinations within 2 working days of that examination for which he or she is absent, failing which they will not be given permission. • **Grade "W":** To a student having satisfactory attendance at classes but withdrawing from that course before the prescribed date in a semester as per Faculty Advice. • **Grade "X":** To a student having attendance ≥85% and CIE ≥ 70%, in a course but SEE performance could result in a 'F' grade in the course. (No "F" grade awarded in this case, but student's performance record will be maintained separately).
22NMT12.17	**The Make Up Examination** facility would be available to students who may have missed to attend the SEE of one or more courses in a semester for valid reasons and given the 'I' grade. Also, students having the 'X' grade shall also be eligible to take advantage of this facility. The makeup examination would be held as per dates notified in the Academic Calendar. However, it should be made possible to hold a make-up examination at any other time in the semester with the permission of the Academic Council of the College. In all these cases, the standard of SEE would be the same as the normal SEE.

<table>
<tr><td>22NMT12.18</td><td>All the 'W' grades awarded to the students would be eligible for conversion to the appropriate letter grades only after the concerned students re-register for these courses in a main/summer semester and fulfil the passing standards for their CIE and (CIE+SEE).</td></tr>
<tr><td>22NMT12.19</td><td>The suggested passing standards are CIE to have >=50% and CIE+SEE to have a grade better or at least equal to C. For maintaining high standards, the students scoring less than 50% in CIE are advised to withdraw and to reregister for the course when offered next. The letter grade ‘W’ to be entered in the grade card against the subject and not to be taken into account while calculating SGPA & CGPA</td></tr>
<tr><td>22NMT12.20</td><td>Rules for grace marks</td></tr>
<tr><td></td><td>Grace marks up to 1% of the maximum total marks of the courses for which he/she is eligible and have registered (non-credit courses excluded) in the examination or 10 marks whichever is less shall be awarded to the failed course(s), (with a restriction of a maximum of 5 marks per course) provided on the award of such grace marks the candidate passes in that course(s).</td></tr>
<tr><td>22NMT13.0</td><td>LETTER GRADES AND GRADE POINTS:
The Institute adopts absolute grading system wherein the marks are converted to grades, and every semester result will be declared with semester grade point average (SGPA) and Cumulative Grade Point Average (CGPA). The CGPA will be calculated for every semester, except for the first semester. The grading system with the letter grades and the assigned range of marks under absolute grading system are as given below:
<table>
<tr><th>Letter Grade</th><th>Grade- Points</th><th>Raw Scores %</th><th>Level of Academic Achievement</th></tr>
<tr><td>O</td><td>10</td><td>≥90</td><td>Out standing</td></tr>
<tr><td>A+</td><td>09</td><td>80-89</td><td>Excellent</td></tr>
<tr><td>A</td><td>08</td><td>70-79</td><td>Very Good</td></tr>
<tr><td>B+</td><td>07</td><td>60-69</td><td>Good</td></tr>
<tr><td>B</td><td>06</td><td>55-59</td><td>Above average</td></tr>
<tr><td>C</td><td>05</td><td>50-54</td><td>Average</td></tr>
<tr><td>F</td><td>00</td><td><50</td><td>Fail</td></tr>
<tr><td>U</td><td></td><td></td><td>Audited</td></tr>
</table>
A student obtaining Grade F in a Course shall be considered fail and is required to reappear in subsequent SEE. Whatever the letter grade secured by the student during his /her reappearance shall be retained. However, the number of attempts taken to clear a Course shall be indicated in the grade cards/</td></tr>
</table>

	transcripts. **Earned Credits:** This refers to the credits assigned to the course in which a student has obtained any one of the letter grades O, A+ A, B+, B and C
22NMT14.0	**PROMOTION AND ELIGIBILITY:**
22NMT14.1	**Promotion:** **a)** All students are promoted to their next semester or year of their program, irrespective of the academic performance. However, for submission for M.Tech. Major Project report in 4th semester, student should have completed all the courses up to 3rd semester
22NMT14.2	**The mandatory non-credit courses,** if any, shall not be considered for the award of class, calculation of SGPA and CGPA. However, a pass grade (PP) in the above courses is mandatory for the award of Degree.
22NMT15.0	**ELIGIBILITY FOR PASSING AND AWARD OF DEGREE:**
22NMT15.1	1. A student who obtains any grade O to C shall be considered as passed and if a student secures F grade in any of the head of passing, he/she has to reappear in that head for SEE. 2. A student shall be declared successful at the end of the program for the award of Degree only on obtaining CGPA≥5.00, with none of the courses remaining with F grade. In case, the CGPA falls below 5.00, the student shall be permitted to appear again for SEE for required number of courses (other than seminar and practical) and times, subject to the provision of University, to make up CGPA≥5.0. The student should reject the SEE results of previous attempt and obtain written permission form the Controller of Examinations to reappear to the subsequent SEE.
22NMT15.2	For a pass in a theory course, the student shall secure a minimum of 40% of the maximum marks prescribed in the Semester End Examination and 50% of marks in CIE and 50% in the aggregate of CIE and SEE marks. The minimum passing grade in a course is C.
22NMT15.3	For a pass in Internship/ Practical/ Project/ Dissertation/ Viva-voce examination, a student shall secure a minimum of 50% of the maximum marks prescribed for the SEE in Internship/ Practical/ Project/ Dissertation/ Viva-voce. The minimum passing grade in a course is C.
22NMT15.4	For a pass, a candidate shall obtain a minimum of 50% of maximum marks in Seminar.

22NMT15.5	IV Semester full time candidates having backlog courses are permitted to upload the dissertation report and to appear for SEE. The IV semester grade card shall be released only when the candidate completes all the backlog courses and become eligible for the award of Degree.
22NMT15.6	**Eligibility for Award of Degree:** A student shall be declared to have completed the Degree of Master of Technology, provided the student has undergone the stipulated course work as per the regulations and has earned the prescribed credits, as per the scheme of teaching and examination of the program
22NMT16.0	**EVALUATION OF PERFORMANCE:** **Computation of SGPA and CGPA** SGPA and CGPA: The credit index can be used further for calculating the Semester Grade Point Average (SGPA) and the Cumulative Grade Point Average (CGPA), both being important academic performance indices of the student. While SGPA is equal to the credit index for a semester divided by the total number of credits registered by the student in that semester, CGPA gives the sum total of credit indices of all the previous semesters divided by the total number of credits registered in all these semesters. Both the equations together facilitate the declaration of academic performance of a student, at the end of a semester and at the end of successive semesters respectively. SGPA is computed as follows: $$SGPA = \frac{\sum[(Course\ Credits) \times (Grade\ Point)]}{\substack{\text{(for all courses with letter grades including F grades in that semester)} \\ \sum[Course\ Credits] \\ \text{(for all courses with letter grades including F grades in that semester)}}}$$ CGPA is computed as follows: $$CGPA = \frac{\sum[(Course\ Credits) \times (Grade\ Point)]}{\substack{\text{(for all courses excluding those with F grades until that semester)} \\ \sum[Course\ Credits] \\ \text{(for all courses excluding those with F grades until that semester)}}}$$
22NMT16.1	**Communication of Grades:** • The SGPA and CGPA respectively, facilitate the declaration of academic performance of a student at the end of a semester and at the end of successive semesters. Both of them would be normally calculated to the second decimal position, so that the CGPA, in particular, can be made use of in rank ordering the students' performance in the Institute. If two students get the same CGPA, the tie could be resolved by considering the number of times a student has obtained higher SGPA, But, if it is still not resolved, the number of times a student has obtained higher grades like O, A,

	B etc. could be taken into account.
22NMT16.2	**Challenge evaluation** If a student is not satisfied with the marks allotted to him/her in the semester end examinations, he/she could apply for challenge evaluation within the prescribed time specified. In such cases the answer papers will be valued by the DPGC committee and marks secured by the students in the challenge evaluation will be final.
22NMT16.3	**Grade Card:** Based on the secured letter grades, grade points, SGPA and CGPA, a grade card for each semester shall be issued. On specific request on paying prescribed fee, a transcript indicating the performance in all semesters may be issued.
22NMT16.4	**Conversions of Grades into Percentage and Class Equivalence** Conversion formula for the conversion of CGPA into percentage is givenbelow: Percentage of marks secured, P = CGPA Earned × 10 **Illustration: for CGPA of 8.18**: P = CGPA Earned 8.18 × 10 = 81.8 %
22NMT17.0	**DEGREE REQUIREMENTS:** The Degree requirements of a student for the M.Tech Degree program are asfollows: 1. College Requirements: i) Minimum Earned Credit Requirement for M.Tech. Degree is 80 ii) Satisfactory completion of all Mandatory Learning courses 2. Program Requirements: i) Minimum Earned Credit Requirements on all core courses, ii) Elective Courses and major project as specified by the DPGC. The maximum duration for a student for complying to the Degree requirements is 8 semesters from the date of first registration for his first semester.
22NMT18.0	**TERMINATION FROM THE PROGRAM/READMISSION:** A student shall be required to leave the College without the award of the Degree, under the following circumstances: i. Failing to complete the degree requirements in double the duration of the program. Based on disciplinary action suggested by the Academic Council/ Governing Council.
22NMT19.0	**GRADUATION REQUIREMENTS AND CONVOCATION:** 1. A student shall be declared to be eligible for the award of the Degree if he has a) Fulfilled Degree Requirements

b) No Dues to the College, Departments, Hostels, Library Central Computer Centre and any other center

c) No disciplinary action pending against him.

2. The award of the Degree must be recommended by the Academic council and approved by Governing Council of Nitte (DU)

Convocation: Degree will be awarded in person for the students who have graduated during the preceding academic year. Degrees will be awarded in absentia to such students who are unable to attend the Convocation. Students are required to apply for the Convocation along with the prescribed fees, after having satisfactorily completed all the Degree requirements within the specified date in order to arrange for the award of the Degree during convocation.

22NMT20.0

AWARD OF CLASS, PRIZES, MEDALS & RANKS:

- **Award of Class:** Sometimes, it would be necessary to provide equivalence of SGPA and CGPA with the percentages and/or Class awarded as in the conventional system of declaring the results of University examinations. This can be done by prescribing certain specific thresholds in these averages for Distinction, First Class and Second Class as described below.

Percentage Equivalence of Grade Points (For a 10-Point Scale)

GPA	Percentage of Marks*	Class
≥ 7.00	≥ 70%	Distinction
≥ 6.00	≥ 60%	First Class
5.0 ≥ GPA <6.00	50≥ Percentage < 60%	Second Class

Percentage * = (GPA) x 10

- **For the award of Prizes, Medals and ranks**: The conditions stipulated by the Donor may be considered as per the statutes framed by the Universityfor such awards.
- An attempt means the appearance/registration of a candidate for an examination in one or more courses either in part or failing a particular examination.
- A candidate who fails/remaining absent (after submitting exam application) in the main examination and passes one or more subjects/courses or all subjects/courses in the supplementary/Make-up examination such candidates shall be considered as taken more than an

	attempt. o Merit Certificates and University Medals/ will be awarded on the basis of overall CGPA, governed by the specific selection criteria that may be formulated by the University for such Medals / Awards o Only those candidates who have completed the Program and fulfilled all the requirements in the minimum number of years prescribed (i.e., 2 years) and who have passed each semester in the first attempt are eligible for the award of Merit Certificates and /or Ranks and University Medals. o Candidates with W, N, I, X & F grades and who passes the courses in the subsequent/supplementary/make up examinations are not eligible for the award of Gold Medal or Merit Certificate.
22NMT21.0	**CONDUCT AND DISCIPLINE:** 1. Students shall conduct themselves within and outside the premises of the Institute, in a manner befitting the students of an Institution of National Importance 2. **As per the order of Honourable Supreme Court of India, ragging in anyform is considered as a criminal offence and is banned, any form of ragging will be severely dealt with**. 3. The following acts of omission/ or commission shall constitute gross Violation of the code of conduct and are liable to invoke disciplinary measures: a) Ragging b) Lack of courtesy and decorum; indecent behaviour anywhere within oroutside the campus. c) Willful damage or stealthy removal of any property /belongings of theInstitute /Hostel or of fellow students/ citizens d) Possession, consumption or distribution of alcoholic drinks or any kind of hallucinogenic drugs. e) Mutilation or unauthorized possession of Library books. f) Noisy and unseemly behavior, disturbing studies of fellow Students. g) Hacking in computer systems (such as entering into other Person's area without prior permission, manipulation and/or Damage of computer hardware and software or any other Cybercrime etc.,). h) Plagiarism of any nature. i) Any other act of gross indiscipline as decided by the University from time to time. j) Smoking in College Campus and supari chewing. k) Unauthorized fund raising and promoting sales. 4. Commensurate with the gravity of offense, the punishment may be reprimand, expulsion from the hostel, debarment from an examination, disallowing the use of certain facilities of the College, rustication for a specified period or even outright expulsion from the College, or even handing over the case to appropriate law enforcement authorities or the judiciary, as required by the circumstances.

	i) For an offence committed in a) A hostel b) A department or in a classroom c) Elsewhere, the Chief Warden, the Head of the Department and the Dean (Students Welfare), respectively, shall have the authority to reprimand or impose fine. ii) All cases involving punishment shall be reported to the principal. 5. Cases of adoption of unfair means and/or any malpractice in an examination shall be reported to the Controller of Examination. ○ **Note:** Students are required to be inside the examination hall 20 minutes before the commencement of examination. This is applicable for all examinations (Semester end/Supplementary/makeup) henceforth. Students will not be allowed inside the examination hall after the commencement, under any circumstances

NITTE (Deemed to be University) | NMAM INSTITUTE OF TECHNOLOGY

Scheme & Syllabus for
M. Tech. (Cyber Security)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

2022-24

M. Tech. in Cyber Security

CREDIT DISTRIBUTION

No.	Course Category	Suggested Credits
1.	Professional Courses (PCC) – core	16
2.	Professional Courses (PEC) – elective	18
3.	Research Methodology & IPR/RETP	04
4.	Labs	04
5.	Project Work (UCC) (Phase 1 & 2)	08+20
6.	Audit Courses	00 (2 Audit Courses)
7.	Seminar on Current Topic (UCC)	02
8.	Internship (UCC)	08
	Total Credits to be earned:	**80**

Program Outcome:

1. An ability to independently carry out research /investigation and development work to solve practical problems.
2. An ability to write and present a substantial technical report/document.
3. Students should be able to demonstrate a degree of mastery over the area as per the specialization ofthe program. (The mastery should be at a level higher than the requirements in the appropriate bachelorprogram)
4. Identify, formally model, define, and solve computing problems by applying the knowledge of mathematical principles, theoretical foundations, and limits of computing.
5. An ability to apply the computational concepts and logics to address a real time problem and to develop software systems, products and processes that are practically feasible to implement using modern tools.
6. An ability to function effectively individually or as a part of a team to accomplish a stated goal.
7. An ability to communicate effectively with a wide range of audience.
8. Recognize the need to engage in self-governing and life-long learning by making use of professional and ethical principles.

Program Specific Outcome (PSO):

- **PSO1.** Acquire the knowledge of logical reasoning and subject fundamentals pertaining to CyberSecurity concepts
- **PSO2.** Apply the concepts of security in cloud computing architecture and adhere to ethicalsecurity behaviour focusing IT compliance and Integrity.

NITTE (Deemed to be University)

NITTE (Deemed to be University) | NMAM INSTITUTE OF TECHNOLOGY

Established under Section 3 of UGC Act 1956
Accredited with 'A+' Grade by NAAC

Off-Campus Centre, Nitte - 574 110, Karkala

M.Tech. (Cyber Security): Scheme of Teaching and Examinations 2022-24

Outcome Based Education (OBE) and Choice Based Credit System (CBCS)

(Effective from the academic year 2022 - 23)

1st Year Scheme

I SEMESTER

Sl. No	Course Type	Course Code	Course Title	Teaching Department	Teaching Hours /Week			Examination				Credits
					Lecture	Tutorial	Practical/ Drawin	Duration in hours	CIEMarks	SEEMarks	Total Marks	
					L	T	P					
1	PCC	22CBS101	Introduction to Cyber Security and Secure Coding	CSE	4	0	0	3	50	50	100	4
2	PCC	22CBS102	Cyber Forensics	CSE	4	0	0	3	50	50	100	4
3	RETP	22CBS103	Research Experience Through Practice -I	CSE	Four contact hours /week for carrying out Research and Interaction between the faculty and students			-	100	0	100	2
4	PCC	22CBS104	Introduction to Cyber Security Lab	CSE	0	0	2	3	50	50	100	1
5	PCC	22CBS105	Cyber Forensics Lab	CSE	0	0	2	3	50	50	100	1
6	PEC	22CBS11X	Elective – I	CSE	3	0	0	3	50	50	100	3
7	PEC	22CBS12X	Elective - II	CSE	3	0	0	3	50	50	100	3
8	PEC	22CBS13X	Elective - III	CSE	3	0	0	3	50	50	100	3
9	AUDIT	22CBSAUXX	Audit Course-I	CSE	2	0	0	0	0	0	0	0
				Total	**19**	**0**	**4**	**21**	**450**	**350**	**800**	**21**

II SEMESTER

Sl. No	Course Type	Course Code	Course Title	Teaching Department	Teaching Hours /Week			Examination				Credits
					Lecture	Tutorial	Practical/ Drawin	Duration in hours	CIEMarks	SEEMarks	Total Marks	
					L	T	P					
1	PCC	22CBS201	Firewall & UTM Architecture	CSE	4	0	0	3	50	50	100	4
2	PCC	22CBS202	AI in Cyber Security	CSE	4	0	0	3	50	50	100	4
3	RETP	22CBS203	Research Experience Through Practice -II	CSE	Four contact hours /week for carrying out Research and Interaction between the faculty and students			-	100	0	100	2
4	PCC	22CBS204	Firewall & UTM Architecture Lab	CSE	0	0	2	3	50	50	100	1
5	PCC	22CBS205	AI in Cyber Security Lab	CSE	0	0	2	3	50	50	100	1
6	PEC	22CBS21X	Elective – IV	CSE	3	0	0	3	50	50	100	3
7	PEC	22CBS22X	Elective – V	CSE	3	0	0	3	50	50	100	3
8	PEC	22CBS23X	Elective – VI	CSE	3	0	0	3	50	50	100	3
9	AUDIT	22CBSAUXX	Audit Course-II	CSE	2	0	0	0	0	0	0	0
				Total	**19**	**0**	**4**	**21**	**450**	**350**	**800**	**21**

Note: PCC: Professional Core Course, PEC: Professional Elective Course, AUDIT (AU): Non-credit Audit course, RETP: Research Experience Through Practice.

L –Lecture, T – Tutorial, P- Practical/ Drawing, CIE: Continuous Internal Evaluation, SEE: Semester End Examination.

NITTE (Deemed to be University) | NMAM INSTITUTE OF TECHNOLOGY

Established under Section 3 of UGC Act 1956
Accredited with 'A+' Grade by NAAC

Off-Campus Centre, Nitte - 574 110, Karkala

M.Tech. (Cyber Security): Scheme of Teaching and Examinations 2022-24

Outcome Based Education (OBE) and Choice Based Credit System (CBCS)

(Effective from the academic year 2022 - 23)

2nd Year Scheme

III SEMESTER												
Sl. No	**Course Type**	**Course Code**	**Course Title**	Teaching Department	**Teaching Hours /Week**			**Examination**				Credits
					Theory Lecture	Tutorial	Practical/ Drawin	Duration in hours	CIEMarks	SEEMarks	Total Marks	
					L	**T**	**P**					
1	UCC	22CBS301	Industry Internship/ Research Internship/Mini Project	CSE	8 Weeks Full Time [32Hrs/week]			3	100	0	100	8
2	UCC	22CBS302	Seminar on Special Topic	CSE	0	0	2	3	100	0	100	2
3	UCC	22CBS303	Project Part -1	CSE	8 Weeks Full Time [32Hrs/week]			3	200	0	200	8
				Total	**0**	**0**	**2**	**9**	**400**	**0**	**400**	**18**
Note: L –Lecture, T – Tutorial, P- Practical/ Drawing, S – Self Study Component, CIE: Continuous Internal Evaluation, SEE: Semester End Examination.												
Internship: CIE Evaluation is for 100 Marks where 50 Marks is for Report and 50 Marks for the Presentation												
Project Part-1: CIE Evaluation is for 200 Marks where 100 Marks is for Report and 100 Marks for the Presentation												

IV SEMESTER												
Sl. No	**Course Type**	**Course Code**	**Course Title**	Teaching Department	**Teaching Hours /Week**			**Examination**				Credits
					Theory Lecture	Tutorial	Practical/ Drawin	Duration in hours	CIEMarks	SEEMarks	Total Marks	
					L	**T**	**P**					
1	UCC	22CBS401	Project Part -2	CSE	20 Weeks Full Time [40Hrs/week]			3	200	200	400	20
				Total	**0**	**0**	**0**	**3**	**200**	**200**	**400**	**20**
Note: L –Lecture, T – Tutorial, P- Practical/ Drawing, S – Self Study Component, CIE: Continuous Internal Evaluation, SEE: Semester End Examination.												
Project Part-2: CIE Evaluation is for 200 Marks having Project Progress Evaluation (PPE)-1 and PPE-2 each for 100 Marks.												

NITTE (Deemed to be University) | NMAM INSTITUTE OF TECHNOLOGY

Established under Section 3 of UGC Act 1956
Accredited with 'A+' Grade by NAAC

Off-Campus Centre, Nitte - 574 110, Karkala

M.Tech. (Cyber Security): Scheme of Teaching and Examinations 2022-24

Outcome Based Education (OBE) and Choice Based Credit System (CBCS)

(Effective from the academic year 2022 - 23)

List of Domain Specific Skill Development Audit Course (AUDIT)	
Course Code	**Course Title**
22CBSAU11	Data Analytics using R Programming
22CBSAU12	Full stack Web Development
22CBSAU13	MOOC Course

List of Electives [PEC]			
Elective - I		**Elective - II**	
Code	**Course Title**	**Code**	**Course Title**
22CBS111	Cloud security & IOT Security	22CBS121	Ethical Hacking and Network Defense
22CBS112	Cyber Security Threats	22CBS122	Cryptography
Elective - III		**Elective - IV**	
Code	**Course Title**	**Code**	**Course Title**
22CBS131	Security Analytics	22CBS211	Malware Analysis and Detection
22CBS132	Secured Network Protocols and Standards	22CBS212	Operating Systems Security
Elective - V		**Elective – VI**	
Code	**Course Title**	**Code**	**Course Title**
22CBS221	Security and Resilience	22CBS231	Cyber security orchestration, automation and simulation
22CBS222	Internet Packet and Application Analysis	22CBS232	Cyber Law

Professional Core Courses

Introduction to Cyber Security and Secure Coding

Course Code:	**22CBS101**	**Course Type**	**PCC**
Teaching Hours/Week (L: T: P)	**4:0:0**	**Credits**	**04**
Total Teaching Hours	**50+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the basics of Cyber Security.
2.	To understand an Enterprise Security Architecture.
3.	To study how to write secure code.
4.	To study how Mathematics concepts are applied in Cyber Security.
5.	To understand and apply the common security threats and how to prevent cyber attacks.

UNIT-I — **12 Hours**

Concepts of Cyber Security, Formal Methods of Security Validation, CIA framework-Confidentiality, Integrity and Authenticity Threat modeling, Types of Cyber Threat.

UNIT-II — **12 Hours**

Concept of secure architecture and system Security, Access Control Mechanisms, Authentication and Information Hiding, data Privacy.

UNIT-III — **08 Hours**

Principles of Security Architecture, Secure Design Steps, Special Design Issues & Bad Practices, Implementation of Good Practices & Bad Practices, Operations Security, Automation and Testing Good General Practices, Lifecycle Risk Assessment Methodologies.

UNIT-IV — **10 Hours**

Implement Secure Programming in Python, C, and Assembly.

UNIT-V — **08 Hours**

Mathematics for Cyber Security:
Elementary Number Theory – Divisibility, Prime numbers, Arithmetic functions, Congruence, Quadratic Residues, Primitive roots, Algorithms for primality testing, Integer Factorization and Discrete Logarithm. Algebraic Structures - Groups, Rings, Fields, and Lattices.

Course Outcomes: At the end of the course student will be able to

1.	Understand the core components of Enterprise Security Architecture.
2.	Define major security risks and how they are mitigated.
3.	Demonstrate the fundamentals of write secure code.
4.	Demonstrate how a secure setup is designed and implemented.
5.	Understand most common mathematical concepts applied in Cyber Security.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	PSO↓	
↓ Course Outcomes							1	2
22CBS101-1.1	x						x	
22CBS101-1.2			x					x
22CBS101-1.3		x					x	
22CBS101-1.4			x					x
22CBS101-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Cryptography and Network Security: Principles and Practice - by William Stallings
2.	Engineering Safe and Secure Software Systems (Artech House Information Security and Privacy - by C. Warren Axelrod
3.	Secure Coding: Principles and Practices – by Mark G. Graff, Kenneth R. van Wyk
4.	Secure Computer Software Development: Introduction to Vulnerability Detection Tools, by Ron McFarland, Ph.D., PMP, CISSP

REFERENCE BOOKS:

1.	Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006
2.	P. K. Saikia, Linear algebra, Pearson Education, 2009.

Cyber Forensics

Course Code:	**22CBS102**	**Course Type**	**PCC**
Teaching Hours/Week (L: T: P)	**4:0:0**	**Credits**	**04**
Total Teaching Hours	**50+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the basics of Cyber Forensics.
2.	To understand and analyze forensic data.
3.	To analyze network logs.
4.	To study cyber laws.
5.	To apply cyber forensic skills to find out malicious users.

UNIT-I — **12 Hours**

Digital forensic evidence collection and processing Framework, Fundamentals of end point forensics for Microsoft windows - Kernel and device driver architecture, Registry, Auditing and security architecture. File system handling - Reconstruction of files and directory structures on the FAT and NTFS.

UNIT-II — **10 Hours**

Fundamentals of host forensics for Unix derivatives - Linux operating system, Kernel and device drives architecture, Security and audit mechanisms, File system and pseudo file systems, Reconstruction of file and directory structures using UFS and EXT2/3/4 file systems as exemplars.

UNIT-III

08 Hours

Forensic analysis of database systems, Database tampering, Forensic analysis of database components, Table storage, Transaction logs, indexes, Forensic recovery for table storage.

UNIT-IV

14 Hours

Network device forensics, investigating logs, Network traffic and web attacks, Mobile device, Social media and wireless forensics, Steganography and image file forensics, Email investigation.

UNIT-V

06 Hours

Cyber laws in India, Case studies and tools.

Course Outcomes: At the end of the course student will be able to

1.	Understand how to perform cyber forensic on Windows devices.
2.	Understand how to perform cyber forensic on Linux devices.
3.	Demonstrate how to capture and analyze network traffic.
4.	Demonstrate how to create a forensic report.
5.	Understand Cyber Laws and latest Cyber Forensic use cases.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→ / **↓ Course Outcomes**	1	2	3	4	5	6	**PSO↓** 1	2
22CBS102-1.1	x						x	
22CBS102-1.2				x				x
22CBS102-1.3		x					x	
22CBS102-1.4			x					x
22CBS102-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition by Gerard Johansen
2.	Brian Carrier, File System Forensic Analysis, Pearson, 2006.
3.	E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2010

REFERENCE BOOKS:

1.	Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations by Niranjan Reddy

Introduction to Cyber Security and Secure Coding Lab

Course Code:	**22CBS104**	**Course Type:**	**PCC Lab**
Teaching Hours/Week (L: T: P)	**0:0:2**	**Credits:**	**01**
Total Teaching Hours:	**0+0+26**	**CIE + SEE Marks:**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To study how to write secure code.
2.	To apply the common security threats and how to prevent cyber attacks.

List of Experiments

1.	Design a sample secure Corporate Network.
2.	Setup Secure Enterprise Infrastructure using Firewall, IDS, LDAP and Log Analytics tool.
3.	Develop sample secure code in Python, C and Assembly language.

Course Outcomes: At the end of the course student will be able to

1.	Develop secure code.
2.	Apply the common security threats and how to prevent cyber attacks.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS104-1.1				x				x
22CBS104-1.2					x		x	

1: Low 2: Medium 3: High

REFERENCE BOOKS:

1.	Secure Coding: Principles and Practices – by Mark G. Graff, Kenneth R. van Wyk
2.	Secure Computer Software Development: Introduction to Vulnerability Detection Tools, by Ron McFarland, Ph.D., PMP, CISSP

Cyber Forensics Lab

Course Code:	**22CBS105**	**Course Type:**	**PCC Lab**
Teaching Hours/Week (L: T: P:)	**0:0:2**	**Credits:**	**01**
Total Teaching Hours:	**0+0+26**	**CIE + SEE Marks:**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand and analyze forensic data.
2.	To apply cyber forensic skills to find out malicious users.

List of Experiments

1.	Collect Forensic data from Windows machine and create report.
2.	Cyber forensic on Linux device.
3.	Perform forensics on MySQL database system.
4.	Capture network data and perform network forensics using Wireshark Tool.

Course Outcomes: At the end of the course student will be able to

1.	Understand and analyze forensic data.
2.	Apply cyber forensic skills to find out malicious users.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS105-1.1				x				x
22CBS105-1.2					x		x	

1: Low 2: Medium 3: High

REFERENCE BOOKS:

1.	Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition by Gerard Johansen.
2.	Brian Carrier, File System Forensic Analysis, Pearson, 2006.
3.	E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2010

Firewall & UTM Architecture

Course Code:	**22CBS201**	**Course Type**	**PCC**
Teaching Hours/Week (L: T: P)	**4:0:0**	**Credits**	**04**
Total Teaching Hours	**50+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the architecture of Firewalls.
2.	To understand the architecture of UTM (Unified threat management).
3.	To study how to plan Firewall deployments.
4.	To configure firewall rules.
5.	To understand and apply the security rules on UTM devices along with IPS and URL Filtering configurations.

UNIT-I — **12 Hours**

Computer and Network Security Concepts and Principles History of Firewalls.

UNIT-II — **12 Hours**

Stateful and Stateless firewalls. Unified Threat Management (UTM) Foundations.

UNIT-III — **10 Hours**

The History of the Unified Threat Management (UTM) Concepts UTM vs other Security Architectures.

UNIT IV — **08 Hours**

UTM vs Next-Generation Firewalls.

UNIT V — **08 Hours**

Best practices while deploying Firewalls in corporate environment.

Course Outcomes: At the end of the course student will be able to

1.	Understand the core components of Next Generation Firewall.
2.	Understand the difference between stateful and stateless firewalls.
3.	Deploy basic firewall along with IPS and URL Filtering feature.
4.	Demonstrate the capabilities of UTM over Basic Firewall.
5.	Able to perform basic Firewall troubleshooting.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS201-1.1	x						x	
22CBS201-1.2			x					x
22CBS201-1.3		x					x	

22CBS201-1.4			x					x
22CBS201-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Official Check Point Administration book (CCSA) - by Check Point Software Technologies.
2.	Learn Wireshark: Confidently navigate the Wireshark interface and solve real-world networking problems - by Lisa Bock.

REFERENCE BOOKS:

1.	Fortigate Firewall Security Pocket Guide (Fortigate Pocket Guide Book 1) – by Ofer shmueli
2.	Fortigate Firewall Security Pocket Guide (Fortigate Pocket Guide Book 2) - by Ofer shmueli

AI in Cyber Security

Course Code:	**22CBS202**	**Course Type**	**PCC**
Teaching Hours/Week (L: T: P)	**4:0:0**	**Credits**	**04**
Total Teaching Hours	**50+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the role of AI and ML in Cyber Security.
2.	To understand identification of latest malwares using AI and ML.
3.	To plan Penetration Testing on Network and Web applications.
4.	To understand Incident Response standard practices.
5.	To apply Cyber Security attack and defense skills in Blue vs Red Game.

UNIT-I — **08 Hours**

AI vs. ML vs. Deep Learning, Detecting Cybersecurity Threats with AI, ML for Cyber Defense, Malware Threat Detection, Network Anomaly Detection with AI.

UNIT-II — **10 Hours**

Malicious hacker insights, OSINT - Maltego, Shodan, Metagoofil , theharvester, Google hacking Database(GHDB)/Google Dorks, Nmap , Nessus vulnerability scanner, Using Metasploit framework, OWASP top 10, Injection Attacks.

UNIT-III — **12 Hours**

Exploiting Redirect vulnerability, Exploiting File Inclusion vulnerability, Exploiting File Upload vulnerability, Exploitation, Port Forwarding & Pivoting, Practical Buffer overflows, Vulnerability Assessment and Management.

UNIT IV — **10 Hours**

Incident Response Fundamentals, Preparing for Incident Response and Handling, Incident Response Processes, Technical Deep Dive with Incident Response Tools, MITRE ATTACK Framework.

UNIT V	
	10 Hours
The Workflow of Incident Response, Networks and Host Attacks, Service and Application Attacks Malicious Code and Insider Threats.	

Course Outcomes: At the end of the course student will be able to

1.	Understand the applied use cases of AI and ML in Cyber Security.
2.	Understand how to perform Penetration Testing of Web Applications.
3.	Understand how to perform Penetration Testing of Database servers.
4.	Demonstrate the various stages of Incident Response.
5.	Understand MITRE ATTACK framework.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS202-1.1	x						x	
22CBS202-1.2			x					x
22CBS202-1.3		x					x	
22CBS202-1.4			x					x
22CBS202-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies by Alessandro Parisi (Author).
2.	Advanced Penetration Testing: Hacking the World's Most Secure Networks by Wil Allsopp.
3.	Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition , 29 January 2020 by Gerard Johansen (Author).

REFERENCE BOOKS:

1.	Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback.

Firewall & UTM Architecture Lab

Course Code:	**22CBS204**	**Course Type:**	**PCC Lab**
Teaching Hours/Week (L: T: P)	**0:0:2**	**Credits:**	**01**
Total Teaching Hours:	**0+0+26**	**CIE + SEE Marks:**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To study how to plan Firewall deployments.

2.	To understand and apply the security rules on UTM devices along with IPS and URL Filtering configurations.

List of Experiments

1.	Design a simple Firewall deployment setup.
2.	Deploy Next Generation Firewall and configure basic settings.
3.	Configure UTM features such as IPS and URL Filtering.
4.	Lab – Learn basic Firewall troubleshooting.

Course Outcomes: At the end of the course student will be able to

1.	Plan Firewall deployments.
2.	Understand and apply the security rules on UTM devices along with IPS and URL Filtering configurations.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22VDE204-1.1				x			x	
22VDE204-1.2				x				x

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Official Check Point Administration book (CCSA) - by Check Point Software Technologies.
2.	Learn Wireshark: Confidently navigate the Wireshark interface and solve real-world networking problems - by Lisa Bock.

REFERENCE BOOKS:

1.	Fortigate Firewall Security Pocket Guide (Fortigate Pocket Guide Book 1) – by Ofer shmueli
2.	Fortigate Firewall Security Pocket Guide (Fortigate Pocket Guide Book 2) - by Ofer shmueli

AI in Cyber Security Lab

Course Code:	**22CBS205**	**Course Type:**	**PCC Lab**
Teaching Hours/Week (L: T: P):	**0:0:2**	**Credits:**	**01**
Total Teaching Hours:	**0+0+26**	**CIE + SEE Marks:**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To plan Penetration Testing on Network and Web applications.
2.	To apply Cyber Security attack and defense skills in Blue vs Red Game.

List of Experiments

1.	Setting up Penetration Testing Environment using open source tools.
2.	Perform Penetration Testing on Web Application and Database server.
3.	Cyber Range Lab for Learning Incident Response in corporate environment.
4.	Cyber Range Lab for Workflow of Incident response.

Course Outcomes: At the end of the course student will be able to

1.	Plan Penetration Testing on Network and Web applications.
2.	Apply Cyber Security attack and defense skills in Blue vs Red Game.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22VDE205-1.1				x			x	
22VDE205-1.2					x			x

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies by Alessandro Parisi (Author).
2.	Advanced Penetration Testing: Hacking the World's Most Secure Networks by Wil Allsopp.
3.	Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition, 29 January 2020 by Gerard Johansen (Author).

REFERENCE BOOKS:

1.	Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter Paperback.

Professional Elective Courses

Cloud security & IOT Security

Course Code:	**22CBS111**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the public and private Infrastructure.
2.	To understand the role of Virtualization in Cloud technologies.
3.	To understand how security is applied in-the-Cloud and of-the-Cloud.
4.	To understand the security risks associated with IOT devices.
5.	To understand and analyze the secure IOT system design.

UNIT-I — **13 Hours**

Fundamentals of Cloud Computing, Cloud Deployment Model, Cloud Delivery and Deployment Architecture, Cloud Shared Responsibility Model, Application of Security Models in IaaS, PaaS, SaaS. Threat Model of a Cloud Architecture, Data Asset Classification and management in a Cloud using CIA Triad, Compute, Storage and Network Assets, Regulatory, Compliance and Legal aspects of Cloud Model, Tagging Cloud Resources.
Lab – Deploy and Secure Virtual Machines on Public Cloud.

UNIT-II — **13 Hours**

Protection of Data in Cloud Environment using Token and Encryption, Key management, Identity and Asset Management, Vulnerability Analysis and Penetration testing in a cloud environment, Tools, Techniques and Procedures for Cloud Security, Introduction of CSA and other cloud Security framework.
Lab – Working with cloud IAM feature.

UNIT-III — **14 Hours**

IoT Reference Model- Functional View, IoT Security Challenges
Hardware Security Risks, Devices Physical Security, Software Security Risks, Lack of Industrial Standards, IoT Security Requirements, Data Confidentiality, Data Encryption, IoT Vulnerabilities, Secret Key, Authentication/Authorization for Smart Devices, Fixed Firmware. IoT Attacks -Side channel Attacks, Reconnaissance, Spoofing Sniffing, Neighbors, Discovery, Rogue Devices, Man-in-Middle, Infrastructure-IPv6 -LowPAN, Bluetooth, LPWAN, Data -MQTT, IoTivity stack, IoT Hardware -Test Device Range-Latency and Capacity -Manufacturability Test -Secure from Physical Attacks, IoT Software -Trusted IoT Application Platforms, -Secure Firmware Updating -Network Enforced Policy -Secure Analytics, Visibility and Control.
Lab – Find security vulnerabilities on given IOT device and create a report.

Course Outcomes: At the end of the course student will be able to

1.	Understand the public and private Infrastructure.
2.	Understand the role of Virtualization in Cloud technologies.
3.	Understand how security is applied in-the-Cloud and of-the-Cloud.

4.	Understand the security risks associated with IOT devices.
5.	Understand and analyze the secure IOT system design.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→ / ↓ Course Outcomes	1	2	3	4	5	6	PSO↓ 1	PSO↓ 2
22CBS111-1.1	x						x	
22CBS111-1.2			x					x
22CBS111-1.3		x					x	
22CBS111-1.4			x					x
22CBS111-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Cloud Computing Security: Foundations and Challenges by John R. Vacca
2.	Cloud Security for Dummies Book by Ted Coombs
3.	Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem, 2nd Edition by Brian Russell and Drew Van Duren

REFERENCE BOOKS:

1.	Mastering Azure Security, by Mustafa Toroman and Tom Janetscheck.
2.	Mastering AWS Security by Albert Anthony
3.	Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment by Sunil Cheruvu, David M. Wheeler, Anil Kumar, Ned Smith

Cyber Security Threats

Course Code:	**22CBS112**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the Security threats.
2.	To analyse Security Threat Management.
3.	Understanding security elements.
4.	Understanding access control.
5.	Understanding human factors.

UNIT-I **14 Hours**

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes. Network Threats: Active/ Passive – Interference – Interception –Impersonation – Worms –Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels –Backdoors – Bots – IP, Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats Environmental threats - Threats to Server security.

UNIT-II	
	14 Hours
Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation –Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools – Threatidentification - Threat Analysis - Threat Modeling - Model for Information Security Planning. Security Elements: Authorization and Authentication - types, policies and techniques – Securitycertification - Security monitoring and Auditing - Security Requirements Specifications – Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots.	
UNIT-III	
	12 Hours
Access control, Trusted Computing and multilevel security - Security models, Trusted Systems,Software security issues, Physical and infrastructure security, Human factors – Security awareness,training , Email and Internet use policies.	

Course Outcomes: At the end of the course student will be able to

1.	To understand the Security threats.
2.	To analyse Security Threat Management.
3.	Understanding security elements.
4.	Understanding access control.
5.	Understanding human factors.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS112-1.1	x						x	
22CBS112-1.2			x					x
22CBS112-1.3		x					x	
22CBS112-1.4			x					x
22CBS112-1.5		x					x	

1: Low 2: Medium 3: High

REFERENCE BOOKS:

1.	Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
2.	William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
3.	Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005.
4.	Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

Ethical Hacking and Network Defense

Course Code:	**22CBS121**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the core concepts of Ethical Hacking.
2.	To understand how security vulnerabilities are exploited.
3.	To analyze the impact of security vulnerabilities in systems.
4.	To understand popular Network Defense solutions deployed at large organizations.
5.	To configure basic firewall and IDS solution.

UNIT-I — **13 Hours**

Fundamentals of Ethical hacking, how organizations gain from Ethical Hacking, Typical Life Cycle of Ethical Hacking, Types of Ethical Hacking- Red, Blue and Purple Teaming, Fundamentals of Vulnerability Analysis and Penetration Testing, Threat Modeling and Attack Surface Identification, Life Cycle of Penetration Testing, Using Kali Linux, and other tools for a penetration testing Assignment.
Lab – Perform Vulnerability and Penetration testing on given Vulnerable system and generate report.

UNIT-II — **13 Hours**

Networking Primer-understanding Security aspect of OSI Model, Active and passive Network Attacks, Network Layer and Cryptography, Single Sign On (SSO), Email encryption: PGP, STARTTLS; IPSec, SSL3.0, TLS 1.2, Attacks on SSL/TLS: Drown attack, Poodle attack, and Secure HTTP, DNSSEC. ARP Cache poisoning, MAC flooding, Port Stealing, DHCP attacks, DNS based attacks, VLAN hopping, Man in the middle attacks. Web Application Security: Security threats, XSS, CSRF, SQL Injection attacks, RFI, DoS/DDoS.

UNIT-III — **14 Hours**

Techniques for Network Intrusion Detection System: Snort, Signature-based and Anomaly-based detection; Firewalls: packet filters and stateful firewalls, application-aware firewalls, Proxies, NAT, VPN, Honeypots and Honeynets.
Lab – Deploy Snort IDS and create custom signatures to capture malicious traffic.

Course Outcomes: At the end of the course student will be able to

1.	To understand how to find security vulnerabilities in given system.
2.	To suggest the remediation steps for identified security bugs.
3.	To perform VAPT task on given system and submit professional report.
4.	To deploy IDS system.
5.	To develop custom IDS signatures.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS121-1.1	x						x	
22CBS121-1.2			x					x
22CBS121-1.3				x				x
22CBS121-1.4			x					x
22CBS121-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:	
1.	The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws Book by Dafydd Stuttard and Marcus Pinto.
2.	Hacking: The Art of Exploitation Book by Jon Erickson.
3.	Hacking Exposed 7: Network Security Secrets and Solutions by Stuart McClure, Joel Scambray, George Kurtz.
4.	Snort Intrusion Detection and Prevention Toolkit by by Brian Caswell, Jay Beale, Andrew Baker.
REFERENCE BOOKS:	
1.	Advanced Penetration Testing: Hacking the World's Most Secure Networks by Wil Allsopp
2.	Snort 2.1 Intrusion Detection, Second Edition by Brian Caswell, Jay Beale (2004), Publisher(s): Syngress

Cryptography

Course Code:	**22CBS122**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the concepts of cryptography.
2.	To study block cipher and their cryptanalysis.
3.	To analyse Symmetric key Encryption.
4.	To understand Message Authentication.
5.	To understand and apply Public Key Encryption.

UNIT-I — **15 Hours**

Introduction to Cryptography, Secure communication, privacy, authenticity, integrity, Why is cryptography hard? Classical Ciphers, One-time pad Shannon's perfect security, Limitation of perfect security.

UNIT-II — **15 Hours**

Block cipher and their cryptanalysis, AES, Pseudo-random functions; Pseudo-random functions II Security Reduction; Modes of Operation; Symmetric key Encryption , Symmetric Key Encryption II, Symmetric Key Encryption III, INC-CCA-Security, Hash Functions, Hash Function II.

UNIT-III — **10 Hours**

Message Authentication Scheme, Authenticated Encryption; Message Authentication II, Computational Number Theory, Computational Number Theory I; Public Key Encryption and El Gamal Public Key Encryption and RSA.

Course Outcomes: At the end of the course student will be able to

1.	Understand the concepts of cryptography.

2.	Analyse block cipher and their cryptanalysis.
3.	Analyse Symmetric key Encryption.
4.	Understand Message Authentication.
5.	Understand and apply Public Key Encryption.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→ / **↓ Course Outcomes**	1	2	3	4	5	6	**PSO↓** 1	2
22CBS122-1.1	x						x	
22CBS122-1.2			x					x
22CBS122-1.3	x						x	
22CBS122-1.4		x					x	
22CBS122-1.5			x				x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	D. Stinson, and the lecture slides by MihirBellare.
2.	D. Stinson Cryptography, Theory and Practice (Third Edition).
3.	M. Bellare Introduction to Modern Cryptography.

REFERENCE BOOKS:

1.	R. Pass and a. shelat. A Course in Cryptography
2.	M. Bellare: Introduction to Modern Cryptography
3.	O. Goldreich. The Foundations of Cryptography

Security Analytics

Course Code:	**22CBS131**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand fundamentals of Security Analytics solution.
2.	To understand the role of SIEM product.
3.	To analyze system (Windows, Linux, Firewall, Routers etc) logs.
4.	To understand the core components of a Security Operations Center (SOC) setup.
5.	To understand how correlation rules are designed and implemented.

UNIT-I — **13 Hours**

Introduction to Security Operations and the SOC, Cybersecurity Challenges, Threat Landscape, Business Challenges, Overview of SOC Technologies.
Lab – Deploy SIEM solution.

UNIT-II — **15 Hours**

Assessing Security Operations Capabilities
SOC Strategy, The SOC Infrastructure, Security Event Generation and Collection, Vulnerability Management, Identifying Vulnerabilities, People and Processes, Technologies to Consider During SOC Design, Firewalls, Preparing to Operate.
Lab - Integrate SIEM solution with Security control devices.

UNIT-III

12 Hours

The Operate Phase, Reacting to Events and Incidents Maintain, Review, and Improve. Practical labs on OSSIM.
Lab – Generate attacks and analyze packets on SIEM solution.

Course Outcomes: At the end of the course student will be able to

1.	To understand the core components of SOC (Security Operation Center).
2.	To understand the architecture of SIEM solution.
3.	To analyze security logs on SIEM solution.
4.	To analyze co-relation rules and alerts.
5.	To understand various dashboards of a SIEM solution.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→ / **↓ Course Outcomes**	1	2	3	4	5	6	**PSO↓** 1	2
22CBS131-1.1	x						x	
22CBS131-1.2		x						x
22CBS131-1.3	x							x
22CBS131-1.4			x				x	
22CBS131-1.5		x					x	

1: Low 2: Medium 3: High3

TEXT BOOKS:

1.	Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder By Don Murdoch GSE
2.	Think Like a Hacker: A Sysadmin's Guide to Cybersecurity By Michael J. Melone and Dr. Shannon Zinck

REFERENCE BOOKS:

1.	Operating and maintaining your SOC by Joey Muniz, Gary McIntyre, Nadhem AlFardan https://linoxide.com/install-configure-alienvault-siem-ossim/

Secured Network Protocols and Standards

Course Code:	**22CBS132**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand network services and applications.
2.	To gain knowledge in multimedia communications and quality of service.
3.	To understand the Security concepts.
4.	To analyse UDP and TCP attacks.
5.	To understand various security standards.

UNIT-I

14 Hours

Network services and applications: DNS, HTTP, SMTP, peer-to-peer systems, Network transport architectures, TCP, UDP, ICMP, TCP congestion control, Routing and forwarding, intra-domain and inter-domain routing algorithms, Link layers and local area networks.

UNIT-II

14 Hours

Ethernet, Wi-Fi, and mobility, Multimedia communications and quality of service, Network measurement, inference, and management, Network experimentation and performance analysis.

UNIT-III

12 Hours

Security: ARP attacks and ARP poisoning, DNS attacks, SYN flood attacks and its mitigation, UDP ping-pong and fraggle attacks, TCP port scanning and reflection attacks; Standards, and Implementing AR & IoT security References.

Course Outcomes: At the end of the course student will be able to

1.	Understand network services and applications.
2.	Gain knowledge in multimedia communications and quality of service.
3.	Understand the Security concepts.
4.	Analyse UDP and TCP attacks.
5.	Understand various security standards.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→ / **↓ Course Outcomes**	1	2	3	4	5	6	**PSO↓** 1	2
22CBS132-1.1	x						x	
22CBS132-1.2		x						x
22CBS132-1.3	x							x
22CBS132-1.4			x				x	
22CBS132-1.5		x					x	

1: Low 2: Medium 3: High

REFERENCE BOOKS:

1.	James F Kurose and Keith W. Ross, "Computer Networking - A Top Down Approach", Fifth Edition, Addison-Wesley, 2010.
2.	L. Peterson and B. Davie, "Computer Networks: A Systems Approach", Fifth Edition, Elsevier Inc., 2011.
3.	W. Richard Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", AddisonWesley,1994.
4.	Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies -Junaid Ahmed Zubairi (SUNY at Fredonia, USA) and AtharMahboob (National University of Sciences & Technology, Pakistan).

Malware Analysis and Detection

Course Code:	**22CBS211**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand different types of malwares.
2.	To understand how malwares can bypass corporate security Infrastructure.
3.	To understand how detection methodologies are applied to catch malwares.
4.	To study latest malware trends.
5.	To deploy basic Malware detection solution using Snort.

UNIT-I — **13 Hours**

The Evolution of the Threat Landscape – Malware, Types of Malwares;
Why is there so much malware on Windows compared to other platforms? Unpatched vulnerabilities, Security misconfigurations.
Lab – Deploy Intrusion detection system using SNORT.

UNIT-II — **13 Hours**

Weak, leaked, and stolen credentials Insider threats, Understanding the difference between the attacker's motivations and tactics.
Lab – Working disassembly using IDA

UNIT-III — **14 Hours**

What is Malware Analysis, Malware Analysis Techniques, Basic Static Analysis, Basic Dynamic Analysis, General Rules for Malware Analysis.
Lab – Debugging Malicious Binaries

Course Outcomes: At the end of the course student will be able to

1.	To understand different types of Malwares.
2.	To understand the approach required to capture Malwares.
3.	To write snort rules to detect malicious traffic.
4.	To perform memory forensics.
5.	To understand how to mitigate Malware threats.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS211-1.1	x						x	
22CBS211-1.2		x						x

22CBS211-1.3	x							x
22CBS211-1.4			x				x	
22CBS211-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition - by Michael Sikorski
2.	Snort Intrusion Detection and Prevention Toolkit Kindle Edition
3.	by Brian Caswell (Author), Jay Beale (Author), Andrew Baker (Author)
4.	Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware 1st ed. Edition,

REFERENCE BOOKS:

1.	Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks 1st Edition, by Tim Rains (Author).
2.	Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, 29 June 2018 by Monnappa K A (Author).

Operating Systems Security

Course Code:	**22CBS212**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the Operating Systems Concepts.
2.	To analyse the Memory Management System
3.	To analyse Windows Management Mechanisms.
4.	To understand access control and file system security.
5.	To analyse Intrusion Detection and Virus Protection.

UNIT-I — **13 Hours**

Operating Systems Concepts – System Calls – OS Organization – Factors in OS Design – Basic Implementation Considerations – Time Sharing and Multi Programming – Real Time Systems. Process Management: Process Concepts, Model – Process Synchronization – Process Scheduling, Threads. Dead Lock: Detection & Recovery, Avoidance, Prevention- Two Phase Locking Issues.

UNIT-II — **13 Hours**

Basic Memory Management – Swapping – Virtual Memory – Page Replacement Algorithms- Segmentation. File System And I/O Management: Files – Low Level File Implementations – Memory Mapped Files – Directories, Implementation – Principles of I/O Hardware & Software – Device Drivers – Disks Hardware, Formatting & Arm Scheduling Algorithms.

UNIT-III — **14 Hours**

The registry, Registry usage, Registry data types, Local structure, Troubleshooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects. Access control and file system security. Remote file system security. NFS, SMB, SFS, User authentication, Passwords, Biometrics, Smartcards. Intrusion Detection and Virus Protection: Trusted Computing, TCPA and NGSCB, Digital Rights Management

Course Outcomes: At the end of the course student will be able to

1.	Understand the Operating Systems Concepts.
2.	Analyse the Memory Management System
3.	Analyse Windows Management Mechanisms.
4.	Understand access control and file system security.
5.	Analyse Intrusion Detection and Virus Protection.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS212-1.1	x						x	
22CBS212-1.2		x						x
22CBS212-1.3	x							x
22CBS212-1.4			x				x	
22CBS212-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Andrew S.Tanenbaum, "Modern Operating Systems", 2nd edition, Addison Wesley, 2001.
2.	Gary Nutt, "Operating Systems A Modern Perspective ", 2nd edition, Pearson Education, 2001.
3.	Maurice J. Bach, "The Design of the Unix Operating System", Prentice Hall of India, 1991.

Security and Resilience

Course Code:	**22CBS221**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the difference between IT and OT security.
2.	To understand basic principles of Effective, Efficient and Cyber Resilient Organizations and Operations
3.	To understand Industrial Control system (ICS) Security framework.

4.	To understand Cyber Resilience best practices in Manufacturing sector.
5.	To gain practical hands-on understanding of Cyber resilience on Cyber Range.

UNIT-I

13 Hours

Effective, Efficient and Cyber Resilient Organizations and Operations; An Insight into Multi-domain Command and Control Systems: Issues and Challenges; Cloud Technologies for Building a System of Data Centers for Defense and Security.

UNIT II

13 Hours

Cyber Situational Awareness in Critical Infrastructure Organizations, Cybersecurity in Next Generation Energy Grids: Challenges and Opportunities for Blockchain and AI Technologies, A New Approach to Assess the Risk of Cyber Intrusion Attacks Over Drones Using Intuitionistic Fuzzy Estimations, Cyber Resilience Using Self-Discrepancy Theory.

UNIT-III

14 Hours

Insider Threats to IT Security of Critical Infrastructures; Empirical Study on Cyber Range Capabilities, Interactions and Learning Features.
Lab – Cyber Range Lab

Course Outcomes: At the end of the course student will be able to

1.	To understand how under cyber resilience in various sectors.
2.	To analyze Cyber Resilience plan of large manufacturing companies.
3.	To understand how latest advancement in technologies are changing the security landscape.
4.	To gain hands on experience working with OT attacks.
5.	To understand key components of Cyber Resiliency Framework.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS221-1.1	x						x	
22CBS221-1.2		x						x
22CBS221-1.3	x							x
22CBS221-1.4			x				x	
22CBS221-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Digital Transformation, Cyber Security and Resilience of Modern Societies: 84 (Studies in Big Data) by Todor Tagarev (Editor), Krassimir T. Atanassov (Editor), Vyacheslav Kharchenko (Editor), Janusz Kacprzyk (Editor)
2.	The Security of Critical Infrastructures: Risk, Resilience and Defense: 288 (International Series in Operations Research & Management Science) by Marcus Matthias Keupp (Editor)

REFERENCE BOOKS:

1.	Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions– 16 September 2016 by Clint Bodungen (Author), Bryan Singer (Author), Aaron Shbeeb (Author), Kyle Wilhoit (Author), Stephen Hilt (Author)
2.	Industrial Cybersecurity: Efficiently secure critical infrastructure systems, 18 October 2017 by Pascal Ackerman (Author)

Internet Packet and Application Analysis

Course Code:	**22CBS222**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand protocols and standards.
2.	To understand optical networking.
3.	To analyse packet switching protocol.
4.	To understand routing in the Internet.
5.	To understand traffic engineering and capacity planning.

UNIT-I — **14 Hours**

Introduction: Protocols and standards, Standards Organizations, Internet Standards, Internet Administration; Overview of reference models: The OSI model, TCP/IP protocol Suite, Addressing, IPversions. Connectors, Transceivers and Media converters, Network Interface cards and PC cards, Repeaters, Hubs, Bridges, Switches, Routers and Gateways etc. H/W selection.

Optical Networking: SONET/SDH standards, Dense Wavelength division multiplexing (DWDM), Performance and design Considerations.

ATM: The WAN Protocol: Faces of ATM, ATM Protocol operations (ATM cell and Transmission) ATM Networking basics, Theory of Operations, B-ISDN reference model, PHY layer, ATM Layer (Protocol model), ATM layer and cell, Traffic Descriptor and parameters, Traffic Congestion control defined, AAL Protocol model, Traffic contract and QoS, User Plane overview, Control Plane AAL, Management Plane,Sub-DS3 ATM, ATM Public services.

UNIT-II — **14 Hours**

Packet Switching Protocol: X.25, theory of Operation and Network Layer functions, X.75, Internetworking protocols, SMDS, Subscriber Interface and Access Protocol, Addressing and Traffic Control. Common Protocols and interfaces in upper Layer: TCP/IP suite, Network Layer, Transport Layer, Applications Layer, Addressing and routing design, Socket programming.

Routing in the Internet: Intra and interdomain routing; UnicastRouting Protocols: RIP, OSPF, BGP; Multicast Routing Protocols: MOSPF, DVMRP. Drawbacks of traditional routing methods, Idea of TE, TE and Different Traffic classes. IP over ATM, Multi protocol Label switching (MPLS), Storage Area Networks (SAN).

UNIT-III — **12 Hours**

Network Management and Services: SNMP: Concept, Management components, SMI, MIB, SNMP format, Messages.

Traffic Engineering and Capacity Planning: Traffic engineering basics: Requirement Definitions: Traffic sizing, characteristics, Protocols, Time Delay considerations, Connectivity, Reliability, Availability and Maintainability, Throughput calculations
Quality of Service: Introduction, Application, Queue Analysis: M/M/1as a packet processing Model, QoS Mechanisms Queue management Algorithms, Feedback, Resource reservation; Queued data and Packet switched traffic modeling. Application and QoS, Network Performance Modeling, Creating Traffic Matrix, Capacity Planning and Network vision, Design Tools.

Course Outcomes: At the end of the course student will be able to

1.	Understand protocols and standards
2.	To understand optical networking.
3.	To analyse packet switching protocol.
4.	To understand routing in the Internet.
5.	To understand traffic engineering and capacity planning.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→ / **↓ Course Outcomes**	1	2	3	4	5	6	**PSO↓** 1	2
22CBS222-1.1	x						x	
22CBS222-1.2		x						x
22CBS222-1.3	x							x
22CBS222-1.4			x				x	
22CBS222-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	B. A. Forouzan, "TCP/IP Protocol Suite", Tata McGraw Hill edition, Third Edition.
2.	N. Olifer, V. Olifer, "Computer Networks: Principles, Technologies and Protocols for Network design", Wiley India Edition, First edition.

REFERENCE BOOKS:

1.	W.Richard Stevens, "TCP/IP Volume1, 2, 3", Addison Wesley
2.	D.E.Comer, "TCP/IP Volume I and II", Pearson Education
3.	W.R. Stevens, "Unix Network Programming", Vol.1, Pearson Education.

Cyber security orchestration, automation and simulation

Course Code:	**22CBS231**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand fundamentals of Security Automation.
2.	To understand the role of SOAR solutions.
3.	To understand the role of BAS (Breach and Attack simulation).
4.	To understand the malware obfuscation techniques.
5.	To understand how to hunt for malwares using Memory forensics.

UNIT-I

Need for Security Automation. Working with APIs. Working with IP addresses, URLs, Hashes and Domains to block attacks automatically. Lab – Setting up lab to automate response by blocking attackers IP on Firewall using API.	**14 Hours**

UNIT-II

Describing the need for SOAR products, Demonstrating SOAR Use Cases, Best practices for SOAR Implementation, Evolution of Breach and Attack Simulation (BAS) devices. Top use cases for BAS solutions.	**14 Hours**

UNIT-III

Malware encoding, Malware encryption and Malware unpacking, Malware hunting using memory forensics, Working with advanced malware using memory forensics. Lab – Working on Memory Forensics tools.	**12 Hours**

Course Outcomes: At the end of the course student will be able to

1.	To demonstrate the need for Security Automation.
2.	To understand the architecture of SOAR deployment.
3.	To analyze the need for BAS solutions.
4.	To understand malware obfuscation tools and techniques.
5.	To analyze malwares using memory forensics tools.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS231-1.1		x					x	
22CBS231-1.2			X					x
22CBS231-1.3	x							x
22CBS231-1.4			x				x	
22CBS231-1.5		x					x	

1: Low 2: Medium 3: High	
TEXT BOOKS:	
1.	Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder By Don Murdoch GSE
2.	Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, 29 June 2018 by Monnappa K A (Author)
REFERENCE BOOKS:	
1.	Security Orchestration For Dummies - Palo Alto Networks

Cyber Law

Course Code:	**22CBS232**	**Course Type**	**PEC**
Teaching Hours/Week (L: T: P)	**3:0:0**	**Credits**	**03**
Total Teaching Hours	**40+0+0**	**CIE + SEE Marks**	**50+50**

Teaching Department: Computer Science and Engineering

Course Objectives:

1.	To understand the need for cyber laws.
2.	To understand the International Perspectives.
3.	To know the Constitutional & Human Rights Issues in Cyberspace.
4.	To understand cybercrimes & legal framework.
5.	To understand Intellectual Property Issues in Cyber Space.

UNIT-I — **12 Hours**

Introduction Computers and its Impact in Society, Overview of Computer and Web Technology, Need for Cyber Law, Cyber Jurisprudence at International and Indian Level.

UNIT-II — **14 Hours**

Cyber Law - International Perspectives UN & International Telecommunication Union (ITU) Initiatives Council of Europe - Budapest Convention on Cybercrime, Asia-Pacific Economic Cooperation (APEC), Organization for Economic Co-operation and Development (OECD), World Bank, Commonwealth of Nations. Constitutional & Human Rights Issues in Cyberspace Freedom of Speech and Expression in Cyberspace, Right to Access Cyberspace – Access to Internet, Right to Privacy, Right to Data Protection.

UNIT-III — **14 Hours**

Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography, Identity Theft, & Fraud Cyber terrorism, Cyber Defamation, Different offences under IT Act, 2000. Cyber Torts Cyber Defamation Different Types of Civil Wrongs under the IT Act, 2000, Intellectual Property Issues in Cyber Space Interface with Copyright Law, Interface with Patent Law, Trademarks & Domain Names Related issues Module VII: E Commerce Concept, E-commerce-Salient Features, Online approaches like B2B, B2C & C2C Online contracts, Click Wrap Contracts, Applicability of Indian Contract Act, 1872. Dispute

Resolution in Cyberspace, Concept of Jurisdiction, Indian Context of Jurisdiction and IT Act, 2000, International Law and Jurisdictional Issues in Cyberspace, Dispute Resolutions.

Course Outcomes: At the end of the course student will be able to

1.	To understand the need for cyber laws.
2.	To understand the International Perspectives.
3.	To know the Constitutional & Human Rights Issues in Cyberspace.
4.	To understand cybercrimes & legal framework.
5.	To understand Intellectual Property Issues in Cyber Space.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**	
↓ Course Outcomes							1	2
22CBS232-1.1	x						x	
22CBS232-1.2		x						x
22CBS232-1.3	x							x
22CBS232-1.4			x				x	
22CBS232-1.5		x					x	

1: Low 2: Medium 3: High

TEXT BOOKS:

1.	Chris Reed & John Angel, Computer Law, OUP, New York, (2007).
2.	Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co, New Delhi, (2012).
3.	Verma S, K, Mittal Raman, Legal Dimensions of Cyber Space, Indian Law Institute, New Delhi, (2004)
4.	Jonthan Rosenoer, Cyber Law, Springer, New York, (1997).

REFERENCE BOOKS:

1.	SudhirNaib, The Information Technology Act, 2005: A Handbook, OUP, New York, (2011)
2.	S. R. Bhansali, Information Technology Act, 2000, University Book House Pvt. Ltd., Jaipur (2003)
3.	Vasu Deva, Cyber Crimes and Law Enforcement, Commonwealth Publishers, New Delhi, (2003)

Audit Courses

Data Analytics using R Programming

Course Code:	**22CBSAU11**	**Course Type:**	**AUDIT**
Teaching Hours/Week (L: T: P)	**1:0:1**	**Credits:**	**-**
Total Teaching Hours:	**13+0+26**	**CIE + SEE Marks:**	**-**

Teaching Department: Computer Science and Engineering

Introduction to R: Handling Packages in R: Installing a R Package, Input and Output – Entering Data from keyboard – Printing fewer digits or more digits, R Data Types, R – Variables, R Operators, R Decision Making, R Loops, R-Function, R-Strings, R Vectors, R List, R Matrices, R Arrays, Data Frames, Expand Data Frame, Loading and handling Data in R; R-CSV Files, R -Excel File; Descriptive Statistics: Data Range, Frequencies, Mode, Mean and Median, Standard Deviation – Correlation - Spotting Problems in Data with Visualization; R – Pie Charts, R Histograms.

Full stack Web Development

Course Code:	**22CBSAU12**	**Course Type:**	**AUDIT**
Teaching Hours/Week (L: T: P)	**1:0:1**	**Credits:**	**-**
Total Teaching Hours:	**13+0+26**	**CIE + SEE Marks:**	**-**

Teaching Department: Computer Science and Engineering

- Requirement analysis and design
- Front end development
- Backend design and development

MOOC Course

Course Code:	**22CBSAU13**	**Course Type:**	**AUDIT**
Teaching Hours/Week (L: T: P)	**1:0:1**	**Credits:**	**-**
Total Teaching Hours:	**13+0+26**	**CIE + SEE Marks:**	**-**

Teaching Department: Computer Science and Engineering

Research Experience Through Practice

RESEARCH EXPERIENCE THROUGH PRACTICE -1

Course Code:	**22CBS103**	**Course Type**	**RETP**
Teaching Hours/Week (L: T: P)	**0:0:4**	**Credits**	**2**
Total Teaching Hours	**0+0+52**	**CIE**	**100**

Teaching Department: Any

Course Objectives: The research purposes are

1. **To foresee future problems through pursuit of truth as a "global centre of excellence for intellectual creativity".**
2. **To respond to current social demands, and to contribute to the creation and development of scientific technologies with the aim of realizing an affluent society and natural environment for humanity.**
3. **At the same time, the course aims to create excellent educational resources and an excellent educational environment through frontline researches**
4. **To Understand professional writing and communication contexts and genres, analyzing quantifiable data discovered by researching, and constructing finished professional workplace documents.**

Individual PG Students are to be allotted to the individual faculty members based on student's area of research interest, specialization of faculty members in the beginning of the first semester.

MODULE -1

Defining the research problem – Selecting the problem – Necessity of defining the problem - Techniques involved in defining the problem – Importance of literature review in defining a problem – Survey of literature – Primary and secondary sources – Reviews, treatise, monographs patents – web as a source – searching the web – Identifying gap areas from literature review – Development of working hypothesis, systematic way of conducting research, write a review / research paper, research proposal, preparation of research report.

MODULE-2

- Introduction various tools related to Cyber Security.
- Introduction to typesetting tool (Latex).
- At the end of the course students should submit a research proposal and should present the idea.

The Research proposal report prepared based on the work carried out by the PG Student is evaluated for 50 marks and 20 minutes presentation on the research work carried out will be evaluated for 50 marks jointly by the examiners.

Course Outcomes: At the end of the course student will be able to

1.	Identify and define the problem statement based on the literature reviewed.
2.	Formulate the objectives specific to the defined problem statement.
3.	Develop the methodology for achieving the objectives.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	**PSO↓**

↓ Course Outcomes							1	2
22CBS103-1.1		x					x	
22CBS103-1.2			x					x
22CBS103-1.3			x				x	

1: Low 2: Medium 3: High

REFERENCE BOOKS:

1.	Gina Wisker, "The Undergraduate Research Hand book", 2018.

E Books / MOOCs/ NPTEL

1.	https://www.classcentral.com/course/swayam-research-methodology-17760

RESEARCH EXPERIENCE THROUGH PRACTICE -2

Course Code:	**22CBS203**	**Course Type**	**RETP**
Teaching Hours/Week (L: T: P)	**0:0:4**	**Credits**	**2**
Total Teaching Hours	**0+0+52**	**CIE**	**100**

Teaching Department: Computer Science and Engineering

Course Objectives: The research purposes are

1. **To foresee future problems through pursuit of truth as a "global centre of excellence for intellectual creativity".**
2. **To respond to current social demands, and to contribute to the creation and development of scientific technologies with the aim of realizing an affluent society and natural environment for humanity.**
3. **At the same time, the course aims to create excellent educational resources and an excellent educational environment through frontline researches.**
4. **To Understand professional writing and communication contexts and genres, analyzing quantifiable data discovered by researching, and constructing finished professional workplace documents.**

The students are expected to carry out Mathematical Modelling/Design calculations/computer simulations/Preliminary experimentation/testing of the research problems identified during Research Experience through Practice-I carried out in the first semester.

At the end of the second semester, students are expected to submit a full research paper based on the Mathematical modelling/Design calculations/computer simulations/Preliminary experimentation/testing carried out during second semester.

The research paper prepared based on the work carried out by the PG Student is evaluated for 50 marks and 20 minutes presentation on the research work carried out will be evaluated for 50marks jointly by the examiners.

Course Outcomes: At the end of the course student will be able to

1.	Create a model/prototype through fabrication, simulation, data analysis, Experimentation for the proposed problem.
2.	Analyse and validate the results obtained.
3.	Compose a technical paper as per the given format.

Course Outcomes Mapping with Program Outcomes & PSO

Program Outcomes→	1	2	3	4	5	6	PSO↓	
↓ Course Outcomes							1	2
22CBS203-1.1		x					x	
22CBS203-1.2			x					x
22CBS203-1.3			x				x	

1: Low 2: Medium 3: High

REFERENCE BOOKS:

1.	Gina Wisker, "The Undergraduate Research Hand book", 2018.

E Resource

1.	https://www.coursera.org/learn/academic-writing-capstone