



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Academic Regulations

(R23) Course Structure & Syllabi

For

Two Year PG Program

in

M. Tech. CSE (Cyber Security)

(Applicable for batches admitted from A.Y. 2023 - 24)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIVERSITY COLLEGE OF ENGINEERING KAKINADA (A)
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
(Established by Andhra Pradesh Act No.30 of 2008)
Kakinada – 533 003, Andhra Pradesh (India)

ACADEMIC REGULATIONS R23 FOR M. Tech (REGULAR) DEGREE COURSE

Applicable for the students of M. Tech (Regular) Course from the Academic Year 2023-24 onwards. The M. Tech Degree of Jawaharlal Nehru Technological University Kakinada shall be conferred on candidates who are admitted to the program and who fulfill all the requirements for the award of the Degree.

1.0 ELIGIBILITY FOR ADMISSIONS

Admission to the above program shall be made subject to eligibility, qualification and specialization as prescribed by the University from time to time.

Admissions shall be made on the basis of merit/rank obtained by the candidates at the qualifying Entrance Test conducted by the University or on the basis of any other order of merit as approved by the University, subject to reservations as laid down by the Govt. from time to time.

2.0 AWARD OF M. Tech DEGREE

2.1 A student shall be declared eligible for the award of the M. Tech Degree, if he pursues a course of study in not less than two and not more than four academic years.

2.2 The student shall register for all 68 credits and secure all the 68 credits.

2.3 The minimum instruction days in each semester are 90.

3.0 A. PROGRAMMES OF STUDY

The following specializations are offered by various departments at present for the M. Tech Programme of study.

Department	Programme
Civil Engg.	1. M.Tech- Structural Engineering 2. M. Tech- Soil Mechanics and Foundation Engineering 3. M.Tech-Water Resource Engineering (UA)
EEE	1. M.Tech- High Voltage Engineering 2. M.Tech- Advanced Electrical Power System 3. M.Tech- Power Electronics and Drives

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

ME	1. M.Tech- CAD/CAM 2. M.Tech- Machine Design 3. M.Tech-Thermal Engineering
ECE	1. M.Tech- Computer and Communication 2. M.Tech- VLSI and Embedded Systems 3. M.Tech- Instrumentation and Control Engineering (UA)
CSE	1. M.Tech- Computer Science and Engineering 2. M.Tech- Artificial Intelligence and Machine Learning 3. M.Tech-Cyber Security

4.0 ATTENDANCE

- 4.1 The faculty handling the course will finalise the attendance as per schedule / before the last instructional day of the course and submit to the Principal through the head of the department.
- 4.2 A student with less than 75% of consolidated attendance (and/or less than 50% in each **and every course**), **will not be permitted to** appear for the end- semester examinations, irrespective of the reason for the shortfall of the attendance. Further, a **student with less than 75% of attendance in Dissertation Phase-2 (IV Semester) will not be permitted to submit his project work.**
- 4.3 The student is however permitted to avail Academic/Medical Leave/ NCC / NSS / Cultural / Sports/ Minor Medical exigencies etc., up to 10% for attending academic related activities like, Industrial Visits, Seminars, Conferences, Competitions etc., with the prior approval of the HoD. After the event, the student should submit the relevant documents for proof to the HoD for approval of the Academic Leave.
- 4.4 **Condonation of shortage of attendance in aggregate up to 10% (65% and above and below 75%, and minimum of 50% in each and every course including laboratory, Dissertation phase-1, Dissertation Phase-2) for a maximum of **ONE time** shall be granted by the College Academic Committee. A prescribed fee shall be payable towards condonation of shortage of attendance.**
- 4.5 Shortage of Attendance below 65% in aggregate shall not be condoned and not eligible to write their end semester examination of that class.
- 4.6 A student shall not be promoted to the next semester unless he satisfies the attendance requirement of the present semester, as applicable. They may seek readmission into that semester when offered next.
- 4.7 If any candidate fulfills the attendance requirement in the present semester, he shall not be eligible for readmission into the same class.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

5.0 EVALUATION

The performance of the candidate in each semester shall be evaluated subject-wise, with a maximum of 100 marks for theory and 100 marks for practical's, on the basis of Internal Evaluation and End Semester Examination.

- 5.1 For the theory subjects 60 marks shall be awarded based on the performance in the End Semester Examination and 40 marks shall be awarded based on the Internal Evaluation. The weightage of Internal marks for 40 consists of Descriptive – 32 and Assignment – 08 (open book exam). Descriptive exam shall be conducted for a total duration of 120 minutes with 4 questions (without choice) each question for 8 marks. The descriptive examination conducted for 32 marks are to be added to the assignment 8 marks for finalizing internal marks for 40. The internal evaluation shall be made based on the average of the marks secured in the two Mid Term-Examinations conducted-one in the middle of the Semester and the other immediately after the completion of instruction. Semester End Exam Paper containing FIVE mandatory questions (one question from one unit) with internal choice, each carrying 12 marks gives for 60marks.
- 5.2 For practical subjects, 60 marks shall be awarded based on the performance in the End Semester Examinations and 40 marks shall be awarded as internal marks, based on the day to day work-10 marks, Record-10 marks and the remaining 20 marks to be awarded by conducting an internal laboratory test. The end examination shall be conducted by the examiners, with a breakup marks of Procedure-15, Experimentation-25, Results-10 ,Viva-voce-10.
- 5.3 For **Mini Project with seminar**, a student under the supervision of a faculty member, shall collect the literature on a topic and critically review the literature and submit it to the department in a report form and shall make an oral presentation before the Project Review Committee consisting of Head of the Department, Supervisor and two other senior faculty members of the department. For Mini Project with seminar, there will be only internal evaluation of 100 marks. A candidate has to secure a minimum of 50% of marks to be declared successful. Out of 100 marks, supervisor awards 40% marks and remaining 60% marks are awarded by the project review committee.
- 5.4 A candidate shall be deemed to have secured the minimum academic requirement in a subject if he secures a minimum of 40% of marks in the End semester Examination and a minimum aggregate of 50% of the total marks in the End Semester Examination and Internal Evaluation taken together. For integrated courses, student should

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

secure the minimum academic requirements in both theory and practical together.

- 5.5 In case the candidate does not secure the minimum academic requirement in any subject (as specified in 5.4) he has to reappear for the End semester Examination in that subject. A candidate shall be given a chance to re-register for each subject provided the internal marks secured by a candidate are less than 50% and has failed in the end examination. In such a case, the candidate must re-register for the subject(s) and secure the required minimum attendance. The candidate's attendance in the re-registered subject(s) shall be calculated separately to decide upon his eligibility for writing the end examination in those subject(s). In the event of the student taking another chance, his internal marks and end examination marks obtained in the previous attempt stand cancelled. For re-registration the candidates have to apply to the college by paying the requisite fees before the start of the semester in which re-registration is required.
- 5.6 In case the candidate secures less than the required attendance in any re registered subject (s), he shall not be permitted to write the End Examination in that subject. He shall again re-register the subject when next offered.
- 5.7 Laboratory examination for M. Tech. programmes must be conducted with two Examiners, one of them being the Laboratory Class Teacher or teacher from the same department and the second examiner shall be appointed by the Principal from the panel of examiners submitted by the respective HoD.
- 5.8 Student is allowed to register for 12 week SWAYAM / NPTEL MOOC courses (recommended by HoD/BoS) and can obtain required credits during II Semester itself. In any case, if a student fails in obtaining credits, he is allowed to repeat the initially opted course / change to another MOOC course or regular course and will be considered as regular candidate only. After successful completion, by end of III/IV Semester, he needs to submit the course certificate (through HoD) to the exam section to perform credit transfer.
- In addition to credit courses, for completing the programme and obtaining degree, a student needs to complete audit courses. Audit courses will be conducted, evaluated as normal credit courses, and the assessment will be graded as Pass/Fail.
- 5.9 Students shall undergo mandatory summer internships (2 credits) for a minimum of eight weeks duration at the end of second semester of the Programme/Summer Break. A student will be required to submit a summer internship report to the concerned department and appear

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

for an oral presentation before the committee. The Committee comprises of Head of the Department and two faculty. The report and the oral presentation shall carry 40% and 60% weightages respectively. For internship, there will be only internal evaluation of 100 marks. A candidate has to secure a minimum of 50% of marks to be declared successful.

6.0 EVALUATION OF PROJECT/DISSERTATION (Phase-I and II):

Every candidate shall be required to submit a thesis or dissertation on a topic approved by the Project Review Committee.

- 6.1 A Project Review Committee (PRC) shall be constituted with Head of the Department and two other senior faculty members in the department.
- 6.2 Registration of Dissertation / Project Work: The work on the project shall be initiated at the beginning of the II year and the duration of the project is two semesters.
- 6.3 A candidate has to submit, in consultation with his project supervisor, the title, objective and plan of action of his project work (published base paper(s) / real time project / industry oriented) for approval. The student can initiate the Project work, only after obtaining the approval from the Project Review Committee (PRC).
- 6.4 If a candidate wishes to change his supervisor or topic of the project, he can do so with the approval of the Project Review Committee (PRC). However, the Project Review Committee (PRC) shall examine whether or not the change of topic/supervisor leads to a major change of his initial plans of project proposal. If yes, his date of registration for the project work starts from the date of change of Supervisor or topic as the case may be.

6.5 A candidate shall present seminar on his project work status in two stages at least with a gap of THREE months between them. If the candidate is absent to any seminar, he should again attend to seminar within two weeks by providing proper evidence to the Project Review Committee for earlier absence to the seminar.

- 6.6 A candidate is permitted to submit Project Thesis (Dissertation) only after successful completion of theory and practical course **with the approval of PRC** not earlier than 40 weeks from the date of registration of the project work.
- 6.7 Continuous assessment of Dissertation-I and Dissertation-II during the Semester will be monitored by the PRC.
- 6.8 There will be pre-submission seminar at the end of academic term.
After the approval the student has to submit the detail report.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

6.9 The Candidate may be permitted to submit the Project Report If only the work is Published/Accepted to be Published in a National or International Journal / conference of reputed and relevance.

- 6.10 Three copies of the Project Thesis certified by the supervisor shall be submitted to the College along with plagiarism report (<40%).
- 6.11 The thesis shall be adjudicated by one examiner selected by the Principal, from the panel of 5 examiners, eminent in that field, submitted by the guide concerned and head of the department.
- 6.12 If the report of the examiner is not favorable, the candidate shall revise and resubmit the Thesis, in the time frame as decided by the PRC. If the report of the examiner is unfavorable again, the thesis shall be summarily rejected. The candidate has to re-register for the project and complete the project within the stipulated time after taking the approval from the Principal.
- 6.13 If the report of the examiner is favorable, Viva-Voce examination shall be conducted by a board consisting of the Supervisor/ Internal examiner, Head of the Department and the examiner who adjudicated the Thesis. The Board shall jointly report the candidate's work for a maximum of 100 Marks. **Out of 100 marks, supervisor awards 40 marks and remaining 60 marks are awarded by the board.**
- 6.14 The Head of the Department shall coordinate and make arrangements for the conduct of Viva-Voce examination.
- 6.15 If the report of the Viva-Voce is unsatisfactory (i.e., <50 marks), the candidate shall retake the Viva-Voce examination only after three months. If he fails to get a satisfactory report at the second Viva-Voce examination, the candidate has to re-register for the project and complete the project within the stipulated time after taking the approval from the Institution.

7.0 Cumulative Grade Point Average (CGPA)

Marks Range (Max – 100)	Letter Grade	Level (G)	Grade Point
≥ 90	>90	Outstanding (O)	10
≥80 to <90	90-80	Excellent (S)	9
≥70 to <80	80-70	Very Good (A)	8
≥60 to <70	70-60	Good (B)	7
≥50 to <60	60-50	Fair (C)	6
<50	<50	Fail (F)	0
		Absent	0

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Computation of SGPA

The following procedure is to be adopted to compute the Semester Grade Point Average (SGPA) and Cumulative Grade Point Average (CGPA):

The **SGPA** is the ratio of sum of the product of the number of credits with the grade points scored by a student in all the courses taken by a student and the sum of the number of credits of all the courses undergone by a student, i.e
$$\text{SGPA (Si)} = \sum (\text{Ci} \times \text{Gi}) / \sum \text{Ci}$$

Where Ci is the number of credits of the i^{th} course and Gi is the grade point scored by the student in the i^{th} course.

Computation of CGPA

The **CGPA** is also calculated in the same manner taking into account all the courses undergone by a student over all the semester of a programme, i.e.
$$\text{CGPA} = \sum (\text{Ci} \times \text{Si}) / \sum \text{Ci}$$

Where Si is the SGPA of the i^{th} semester and Ci is the total number of credits in that semester. The SGPA and CGPA shall be rounded off to TWO decimal points and reported in the transcripts.

8.0 AWARD OF DEGREE AND CLASS

After a student has satisfied the requirements prescribed for the completion of the program and is eligible for the award of M. Tech. Degree he shall be placed in one of the following four classes:

Class Awarded	CGPA to be secured	From the CGPA secured from 68 Credits.
First Class with Distinction	≥ 7.75 without backlog history	
First Class	≥ 6.75	
Second Class	≥ 5.75 to < 6.75	

The secured grade, grade points, status and credits obtained will be shown separately in the memorandum of marks.

WITHHOLDING OF RESULTS

If the student has not paid the dues, if any, or if any case of indiscipline is pending against him, the result of the student will be withheld. His degree will be withheld in such cases.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

9.0 TRANSITORY REGULATIONS

- 9.1 Discontinued or detained candidates are eligible for re-admission into same orequivalent subjects at a time as and when offered.

10. GENERAL

- 10.1 Wherever the words “he”, “him”, “his”, occur in the regulations, they include “she”, “her”, “hers”.
- 10.2 The academic regulation should be read as a whole for the purpose of any interpretation.
- 10.3 In the case of any doubt or ambiguity in the interpretation of the above rules, the decision of the Vice-Chancellor is final.
- 10.4 The College may change or amend the academic regulations or syllabi at any time and the changes or amendments made shall be applicable to all the students with effect from the dates notified by the College.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

MALPRACTICES RULES

DISCIPLINARY ACTION FOR / IMPROPER CONDUCT IN EXAMINATIONS

	Nature of Malpractices/ Improper conduct	Punishment
	<i>If the candidate:</i>	
1. (a)	Possesses or keeps accessible in examination hall, any paper, note book, programmable calculators, Cell phones, pager, palm computers or any other form of material concerned with or related to the subject of the examination (theory or practical) in which he is appearing but has not made use of (material shall include any marks on the body of the candidate which can be used as an aid in the subject of the examination)	Expulsion from the examination hall and Cancellation of the performance in that subject only.
(b)	Gives assistance or guidance or receives it from any other candidate orally or by any other body language methods or communicates through cell phones with any candidate or persons in or outside the exam hall in respect of any matter.	Expulsion from the examination hall and cancellation of the performance in that subject only of all the candidates involved. In case of an outsider, he will be handed over to the police and a case is registered against him.
2	Has copied in the examination hall from any paper, book, programmable calculators, palm computers or any other form of material relevant to the subject of the examination (theory or practical) in which the candidate is appearing.	Expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted to appear for the remaining examinations of the subjects of that Semester/year.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

3.	Impersonates any other candidate in connection with the examination.	The candidate who has impersonated shall be expelled from examination hall. The candidate is also debarred and forfeits the seat. The performance of the original candidate who has been impersonated, shall be cancelled in all the subjects of the examination (including practical and project work) already appeared and shall not be allowed to appear for Examinations of the remaining subjects of that semester/year. The candidate is also debarred for two consecutive semesters from class work and all External examinations. The continuation of the course by the candidate is subject to the academic regulations in connection with forfeiture of seat. If the imposter is an outsider, he will be handed over to the police and a case is registered against him.
4.	Smuggles in the Answer book or additional sheet or takes out or arranges to send out the question paper during the examination or answer book or additional sheet, during or after the examination.	Expulsion from the examination hall and cancellation of performance in that subject and all the other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred for two consecutive semesters from class work and all External examinations. The continuation of the course by the candidate is subject to the academic regulations in connection with forfeiture of seat.
5.	Uses objectionable, abusive or offensive language in the answer paper or in letters to the examiners or writes to the examiner requesting him to award pass marks.	Cancellation of the performance in that subject.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

6.	Refuses to obey the orders of the Chief Superintendent/Assistant-Superintendent / any officer on duty or misbehaves or creates disturbance of any kind in and around the examination hall or organizes a walk out or instigates others to walk out, or threatens the officer-in charge or any person on duty in or outside the examination hall of any injury to his person or to any of his relations whether by words, either spoken or written or by signs or by visible representation, assaults the officer-in-charge, or any person on duty in or outside the examination hall or any of his relations, or indulges in any other act of misconduct or mischief which result in damage to or destruction of property in the examination hall or any part of the College campus or engages in any other act which in the opinion of the officer on duty amounts to use of unfair means or misconduct or has the tendency to disrupt the orderly conduct of the examination.	In case of students of the college, they shall be expelled from examination halls and cancellation of their performance in that subject and all other subjects the candidate(s) has (have) already appeared and shall not be permitted to appear for the remaining examinations of the subjects of that semester/year. The candidates also are debarred and forfeit their seats. In case of outsiders, they will be handed over to the police and a police case is registered against them.
7.	Leaves the exam hall taking away answer script or intentionally tears of the script or any part thereof inside or outside the examination hall.	Expulsion from the examination hall and cancellation of performance in that subject and all the other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred for two consecutive semesters from class work and all External examinations. The continuation of the course by the candidate is subject to the academic regulations in connection with forfeiture of seat.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

8.	Possess any lethal weapon or firearm in the examination hall.	Expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred and forfeits the seat.
9.	If student of the college, who is not a candidate for the particular examination or any person not connected with the college indulges in any malpractice or improper conduct mentioned in clause 6 to 8.	Student of the colleges expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester/year. The candidate is also debarred and forfeits the seat. Person(s) who do not belong to the College will be handed over to police and, a police case will be registered against them.
10.	Comes in a drunken condition to the examination hall.	Expulsion from the examination hall and cancellation of the performance in that subject and all other subjects the candidate has already appeared including practical examinations and project work and shall not be permitted for the remaining examinations of the subjects of that semester /year.
11.	Copying detected on the basis of internal evidence, such as, during valuation or during special scrutiny.	Cancellation of the performance in that subject and all other subjects the candidate has appeared including practical examinations and project work of that semester/year examinations.
12.	If any malpractice is detected which is not covered in the above clauses 1 to 11 shall be reported to the University for further action to award suitable punishment.	

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Examination Branch
Appointment of Subject Expert for QP Setting

From
Dr U V Ratna Kumari
Vice-Principal

Date: 01.10.2023.

To

I am advised to inform you that you are appointed as subject expert to set the question paper(s) as per the details noted below. You are requested to set the question paper(s) in MS word document format and send a soft copy oiel.ucek@jntucek.ac.in. The hard copies of the question paper(s) shall be sent along with the remuneration bill.

You are requested to set the Question Paper(s) by following OBE pattern, as per the revised Bloom's Taxonomy herewith enclosed. Keep this appointment strictly confidential.

1. You are requested to prepare a balanced question paper within the prescribed syllabus covering the entire syllabus. The duration of the examination is **3-hours** and you are requested to prepare the questions in such a way that student must be able to answer each question for about 35-45 minutes time.
2. It is informed that the question paper covering the topics of all FIVE units for 60 marks. Also the question paper shall be set as per the format enclosed, containing ten main questions (two from each unit) over FIVE-units of syllabus with internal choice and **12marks** for each question. The main question shall contain sub questions like 1(a), 1(b) etc.
3. The student has to answer FIVE mandatory questions (One question from one unit).
4. The requirement of data books, codes, graphs etc. may please be indicated on the question paper.
5. You are requested to give the distribution of the marks for each question.
- 6. You are requested not to reproduce questions from previous question papers.**
7. Remuneration for setting of one question paper for M.Tech(PG) programme is **Rs. 1,200/-** per set.
8. You are requested to confirm your acceptance through e-mail.

You are requested to reject the offer and intimate the same to the Vice Principal, if any of your relatives are writing the examination or if you are involved in any extra assignment in any tutorial/coaching centers. Please send the question paper in the enclosed model (model is attached for reference).

Question Paper Details		R19 OBE Pattern			
Course	M.Tech (PG)	Question No.	Unit/CO's	Bloom's Taxonomy Level	Marks
Name of the Examination	I-M.Tech, I-Sem (R23) Regular End Exams, Dec-2023	I	U1/CO1	L2/L3/L4	12
Subjects	XXXXXXX	II	U2/CO2	L2/L3/L4	12
Branch	XXXXXXXXXX	III	U3/CO3	L2/L3/L4	12
No of Question Paper Sets	1 (Ono)	IV	U4/CO4	L2/L3/L4	12
Last Date for submission	14/11/2023	V	U5/CO5	L2/L3/L4	12

Note: U1: Unit 1, CO1: Course Outcome 1

L1: Level 1(Bloom's Cognitive Level) L2: Understanding Level; L3: Apply Level; L4: Analyze Level.

VICE-PRINCIPAL



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Course Code:

R23

University College of Engineering Kakinada (Autonomous)
Jawaharlal Nehru Technological University Kakinada

() B. Tech. () Semester (R23) Regular Examinations, ()

COURSE NAME
(NAME OF BRACH)

Time: 3 hrs.

Max Marks: 60

Answer all five questions

5X12=60

Q.No	Question	Marks	CO	BL
UNIT-1				
1(a)				
1(b)				
(OR)				
2(a)				
2(b)				
UNIT-2				
3(a)				
3(b)				
(OR)				
4(a)				
4(b)				
UNIT-3				
5(a)				
5(b)				
(OR)				
6(a)				
6(b)				
UNIT-4				



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

7(a)				
7(b)				
(OR)				
8(a)				
8(b)				
UNIT-5				
9(a)				
9(b)				
(OR)				
10(a)				
10(b)				

Note: CO: Course Outcome, BL: Bloom's Cognitive Level;

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

REVISED Bloom's Taxonomy Action Verbs

Definitions	I. Remembering	II. Understanding	III. Applying	IV. Analyzing	V. Evaluating	VI. Creating
Bloom's Definition	Exhibit memory of previously learned material by recalling facts, terms, basic concepts, and answers.	Demonstrate understanding of facts and ideas by organizing, comparing, translating, interpreting, giving descriptions, and stating main ideas.	Solve problems to new situations by applying acquired knowledge, facts, techniques and rules in a different way.	Examine and break information into parts by identifying motives or causes. Make inferences and find evidence to support generalizations.	Present and defend opinions by making judgments about information, validity of ideas, or quality of work based on a set of criteria.	Compile information together in a different way by combining elements in a new pattern or proposing alternative solutions.
Verbs	<ul style="list-style-type: none"> Choose Define Find How Label List Match Name Omit Recall Relate Select Show Spell Tell What When Where Which Who Why 	<ul style="list-style-type: none"> Classify Compare Contrast Demonstrate Explain Extend Illustrate Infer Interpret Outline Relate Rephrase Show Summarize Translate 	<ul style="list-style-type: none"> Apply Build Choose Construct Develop Experiment with Identify Interview Make use of Model Organize Plan Select Solve Utilize 	<ul style="list-style-type: none"> Analyze Assume Categorize Classify Compare Conclusion Contrast Discover Dissect Distinguish Divide Examine Function Inference Inspect List Motive Relationships Simplify Survey Take part in Test for Theme 	<ul style="list-style-type: none"> Agree Appraise Assess Award Choose Compare Conclude Criteria Criticize Decide Deduct Defend Determine Disprove Estimate Evaluate Explain Importance Influence Interpret Judge Justify Mark Measure Opinion Perceive Prioritize Prove Rate Recommend Rule on Select Support Value 	<ul style="list-style-type: none"> Adapt Build Change Choose Combine Compile Compose Construct Create Delete Design Develop Discuss Elaborate Estimate Formulate Happen Imagine Improve Invent Make up Maximize Minimize Modify Original Originate Plan Predict Propose Solution Solve Suppose Test Theory

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

M. Tech. (CY) I SEMESTER							
S.No	Course Code	Courses	Cate gory	L	T	P	C
1	R23MCY1151	Program Core-1 (Integrated Course-Theory & Laboratory Course) Cyber Security	PC	3	0	3	4.5
2	R23MCY1152	Program Core-2 Cryptography	PC	3	0	0	3
3	R23MCY1153	Program Elective-1 1. Operating Systems Administration and Security 2. Cyber Laws and Security Policies 3. Cloud and IoT Security 4. ML Applications to Security	PE	3	0	0	3
4	R23MCY1154	Program Elective-2 1. Networks Security 2. Cyber Security Operations and Design 3. Database and Web Applications Security 4. Block Chain Technologies	PE	3	0	0	3
5	R23MCY1155	Research Methodology and IPR	CC	2	0	0	2
6	R23MCY1156	Laboratory-1 Cryptography Lab	LB	0	0	3	1.5
7	R23MCY1157	Audit Course-1* 1. English for Research Paper Writing 2. Disaster Management 3. Sanskrit for Technical Knowledge 4. Value Education	AC	2	0	0	0
Total Credits							17

**Student has to choose any one audit course listed.*



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

M. Tech. (CY) II SEMESTER							
S.No	Course Code	Courses	Category	L	T	P	C
1	R23MCY1251	Program Core-3 (Integrated Course-Theory & Laboratory Course) Cyber Crime Investigation and Digital Forensics	PC	3	0	3	4.5
2	R23MCY1252	Program Core-4 Web Security	PC	3	0	0	3
3	R23MCY1253	Program Elective-3 1. Software Vulnerability Analysis 2. Malware Analysis and Reverse Engineering 3. Application Threat Detection 4. Information System Audit	PE	3	0	0	3
4	R23MCY1254	Program Elective-4 1. Biometric Security 2. AI in Cyber Security 3. Ethical Hacking 4. Risk Management	PE	3	0	0	3
6	R23MCY1255	Laboartory-2 Web Security Lab	LB	0	0	3	1.5
7	R23MCY1256	Mini Project with Seminar	MP	2	0	0	2
8	R23MCY1257	Audit Course-2 * 1. Constitution of India 2. Pedagogy Studies 3. Stress Management by Yoga 4. Personality Development through Life Enlightenment Skills etc	AC	2	0	0	0
Total Credits							17

**Student has to choose any one audit course listed.*

**Students are encouraged to go to Industrial Training/ Internship for at least 2-3 months during semester break*



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

M. Tech. (CY) III SEMESTER							
S.No	Course Code	Courses	Category	L	T	P	C
1	R23MCY2151	Program Elective-5 1. Cyber Security Governance 2. Principles of Secure Coding 3. Security Automation 4. MOOCs-1 (NPTEL/ SWAYAM) 12 Week Program related to the program which is not listed in the course structure (PG Level)	PE	3	0	0	3
2	R23MCY2152	Open Elective 1. MOOCs (NPTEL/SWAYAM)-Any 12 Week Course on Engineering/ Management/ Mathematics offered by other than parent department 2. Course offered by other departments in the college	OE	3	0	0	3
3	R23MCY2153	Internship (During II Sem to III Sem / Summer break in I Year - 6 to 8 weeks internship)					2
4	R23MCY2154	Dissertation-I/Industrial Project	PJ	0	0	20	10
		Total Credits					18

*Students going for Industrial Project/Thesis will complete these courses through MOOCs



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

M. Tech. (CY) IV SEMESTER							
S.No	Course Code	Courses	Category	L	T	P	C
1	R23MCY2251	Dissertation-II	PJ	0	0	32	16
Total Credits							16



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Cyber Security (R23MCY1151)	L	T	P	C
		3	0	3	4.5

Course Objectives:

- To learn threats and risks within context of the cyber security architecture.
- Student should learn and Identify security tools and hardening techniques.
- To learn types of incidents including categories, responses and timelines for response.

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

Course Outcomes		Knowledge Level (K)#
C01	Apply cyber security architecture principles.	K3
C02	Demonstrate the risk management processes and practices.	K2
C03	Appraise cyber security incidents to apply appropriate response	K5
C04	Distinguish system and application security threats and vulnerabilities.	K4
C05	Identify security tools and hardening techniques	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction to Cyber Security-Cyber security objectives, roles, differences between information security and cyber security, Cyber security principles-confidentiality, integrity, availability, authentication and non repudiation

UNIT-II: Information Security within Lifecycle Management-Lifecycle management landscape, Security architecture processes, Security architecture tools, Intermediate lifecycle management concepts, **Risks & Vulnerabilities**-Basics of risk management, Operational threat environments, Classes of attacks



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-III: Incident Response-Incident categories, Incident response, Incident recovery, **Operational security protection**-Digital and data assets, ports and protocols, Protection technologies, Identity and access Management, configuration management

UNIT-IV: Threat Detection and Evaluation Monitoring-Vulnerability management, Security logs and alerts, Monitoring tools and appliances, **Analysis**-Network traffic analysis, packet capture and analysis

UNIT-V: Introduction to backdoor System and security-Introduction to metasploit, backdoor, demilitarized zone (DMZ), Digital signature, Brief study on Hardening of operating system.

List of Experiments:

1. Program to check vulnerabilities in web applications.
2. Analysis of network traffic using packet capturing tools.
3. Identify the open, close ports and protocols using tools.
4. Identify the vulnerabilities in a network.
5. Establishment of demilitarized zone.
6. Hardening of operating system.
7. Manually disabling unnecessary services and ports and locking down the ports.
8. Implementation of in-bound and out-bound rules in a client system.
9. Report bugs in any web application using tool.
10. Program to implement metasploit in windows or Linux.
11. Implementation of Incident response with tools.
12. Identifying the vulnerable logs in windows system
13. Generate digital certificates using tools.
14. Establish a backdoor on the target machine via pivot points
15. Implementation of patch Management in client system.

Text Books:

1. NASSCOM: Security Analyst Student Hand Book, Dec 2015
2. Information Security Management Principles, Updated Edition, David Alexander, Amanda Finch, David Sutton, BCS publishers, June 2013

Reference Books:

1. Cyber Security Fundamentals-Cyber Security, Network Security and Data Governance Security, 2nd Edition, ISACA Publishers, 2019

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Cryptography (R23MCY1152)	L	T	P	C
		3	0	0	3

Course Objectives:

1. To understand the fundamentals of Cryptography
2. To understand various key distribution and management schemes
3. To understand how to deploy encryption techniques to secure data in transit across data networks
4. To apply algorithms used for secure transactions in real world applications

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

Course Outcomes		Knowledge Level (K)#
C01	Demonstrate the knowledge of cryptography, network security concepts and applications.	K2
C02	Apply security principles in system design	K3
C03	Identify and investigate vulnerabilities and security threats and mechanisms to counter them	K3
C04		
C05		

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT – I:

INTRODUCTION: Security trends, The OSI Security Architecture, Security Attacks, Security Services and Security Mechanisms, A model for Network security.

CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Modes, Substitute Techniques, Transposition Techniques, Stenography

UNIT – II:

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

BLOCK CIPHER AND DATA ENCRYPTION STANDARDS: Block Cipher Principles, Data Encryption Standards, the Strength of DES, Block Cipher Design Principles.

ADVANCED ENCRYPTION STANDARDS: Evaluation Criteria for AES, the AES Cipher.

MORE ON SYMMETRIC CIPHERS: Multiple Encryption, Triple DES, Block Cipher Modes of Operation, Stream Cipher and RC4.

UNIT – III:

Number Theory: Preliminaries, Modular arithmetic, elementary group theory, CRT, hardness assumptions.

PUBLIC KEY CRYPTOGRAPHY AND RSA: Principles Public key crypto Systems the RSA algorithm, Key Management, Diffie Hellman Key Exchange.CCA secure public key encryption

HASH FUNCTIONS:Pseudo-random Generators, (Strong) Pseudo-random Functions (Permutations) Hash Function, Security of Hash Function and MACs.

UNIT – IV:

HASH AND MAC ALGORITHM: Secure Hash Algorithm, Whirlpool, HMAC, CMAC. DIGITAL SIGNATURE: Digital Signature, Authentication Protocol, Digital Signature Standard

FIREWALL: Firewall Design principles, Types of firewalls, Trusted Systems.

UNIT – V:

Hardware Security: HSM Hardware Security Module -Introduction, Benefits of HSM , HSM- Use Cases , HSM Software –Card sets and Keys,Key Protection and Key Creation,Next Generation of HSM

Text Books:

1. William Stallings (2006), Cryptography and Network Security: Principles and Practice, 4th edition, Pearson Education, India.
2. William Stallings (2000), Network Security Essentials (Applications and Standards), Pearson Education, India.
3. [Gerardus Blokdyk](#) (2018) *Hardware security module* A Clear and Concise Reference,5starcooks

Reference Books:

1. Charlie Kaufman (2002), Network Security: Private Communication in a Public World, 2nd edition, Prentice Hall of India, New Delhi.
2. Atul Kahate (2008), Cryptography and Network Security, 2nd edition, Tata Mc Grawhill, India.
3. Robert Bragg, Mark Rhodes (2004), Network Security: The complete reference, Tata Mc Grawhill, India.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Operating Systems Administration and Security (R23MCY1153)	L	T	P	C
		3	0	0	3

Course Objectives:

- Students will learn and apply basic concepts and methodologies of System Administration and Security by building from the ground up a miniature corporate network.
- To know some basic security measures to take in system administration.
- To prepare for possible disasters, including an understanding of backup and restoration of file systems.

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

Course Outcomes		Knowledge Level (K)#
C01	Explain the important computer system resources and the role of operating system in their management policies and algorithms.	K2
C02	Describe the concepts of Access control Fundamentals, Multics.	K4
C03	Identify and assess current and anticipated security risks and vulnerabilities.	K3
C04	Identify the security Techniques and apply the real time applications.	K3
C05	Explain the role and responsibilities of a system administrator and Create and administer user accounts on both a Linux and Windows platform.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Overview of Operating Systems-Introduction, Computer system organization and architecture, Operating system structure and operations, Process Management, Memory Management, file systems management Protection and security, Scheduling Algorithms, Inter-process Communication(Text Book1)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-II: Operating Systems Protection: Protection Goals, Protection Threats, Access Control Matrix, Access Control Lists(ACL's), Capability Lists(C-lists), Protection systems, Lampson's access matrix, mandatory protection systems, Reference monitor, Secure operating system definition(Text Book 2)

UNIT-III: Operating System Security-Security Goals, Security Threats, Security Attacks- Trojan Horses, Viruses and Worms, Buffer Overflow attacks and Techniques, Formal Aspects of Security, Encryption- Attacks on Cryptographic Systems, Encryption Techniques, Authentication and Password Security, Intrusion detection, malware defences, UNIX and Windows security(Text Book 2)

UNIT-IV: System Administration: Security Basics, Securing the Server Itself, Maintenance and Recovery, Monitoring and Audit, Introduction to Linux Systems, Configuration Management, Log Auditing and Vulnerability Assessment.(Text Book 3)

UNIT-V: Linux Networking: Networking Technologies: DHCP, DNS, NFS/iSCSI, SMTP, SNMP, LAMP, Firewall/IDS/SSH, Securing Linux. **Case Studies:** Security and Protection-MULTICS, UNIX, LINUX and Windows, Windows and Linux Coexisting.(Text Book 4)

Text Books:

1. Operating System Concepts, 9th Edition, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley Publication, 2008
2. Advanced Concepts in Operating Systems, 1st Edition, Mukesh Singhal and N. G. Shivaratri, McGraw- Hill, 2000

Reference Books:

1. Operating System: Internals and Design Principles, 7th Edition, William Stalling, Prentice Hall, 2012
2. An Introduction to Operating Systems: Concepts and practice, 4th Edition, Promod Chandra P Bhat, Prentice Hall of India, 2014
3. Linux System Administration, Tom Adelstein and Bill Lubanovic, 1st Edition, O'Reilly Media, Inc., 2009

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Cyber Laws and Security Policies (R23MCY1153)	L	T	P	C
		3	0	0	3

Course Objectives:

- To Enable Learner To Understand, Explore, And Acquire A Critical Understanding Cyber Law.
- Student learns and develops Competencies for Dealing with Frauds and Deceptions (Confidence Tricks, Scams) And Other Cyber Crimes For Example, Child Pornography Etc. That Are Taking Place Via The Internet.
- Student should learn security policies and procedures.

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

Course Outcomes		Knowledge Level (K)#
C01	Design the Social And Intellectual Property Issues Emerging From Cyberspace.	K6
C02	Explain The Legal And Policy Developments In Various Countries To Regulate Cyberspace	K2
C03	Develop The Understanding Of Relationship Between Commerce And Cyberspace.	K3
C04	Determine in Depth Knowledge Of Information Technology Act And Legal Frame Work Of Right To Privacy, Data Security And Data Protection.	K5
C05	Apply various Case Studies On Real Time Crimes.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-I: Introduction to Computer Security- Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

UNIT-II: Secure System Planning and administration- Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, and Network Security, The Redbook and Government network evaluations.

UNIT-III: Information security policies and procedures-Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies- asset classification policy- developing standards.

UNIT-IV: Information security-fundamentals-Employee responsibilities- information classification- Information handling- Tools of information security- Information processing-secure program administration.

UNIT-V: Organizational and Human Security-Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals, IT Act- Structure of IT Act, Common cyber crime scenarios and Applicability of Legal sections, Case studies as per selected IT Act sections.

Text Books:

1. Computer Security Basics (Paperback), 2nd Edition, Debby Russell and Sr. G.T Gangemi, O'Reilly Media, 2006
2. Information Security policies and procedures: A Practitioner's Reference, 2nd Edition, Thomas R. Peltier Prentice Hall, 2004

Reference Books:

1. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, Kenneth J. Knapp, IGI Global, 2009

Web References:

1. <https://meity.gov.in/content/information-technology-act 2000>

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Cloud and IoT Security (R23MCY1153)	L	T	P	C
		3	0	0	3

Course Objectives:

- Student learn and understand the advantages, challenges, security issues of cloud computing and interrelationships between cloud computing and big data.
- Student learns different Key components of Amazon Web Services, Cloud Backup and solutions.
- Student able to discuss the main threats and attacks on IoT products and services
- Be able to learn secure a connected IoT product from scratch.

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

Course Outcomes		Knowledge Level (K)#
CO1	Analyze the Cloud Computing and the different Cloud services and deployment models	K4
CO2	Assessing the financial, technological, and organizational capacity of employer's for actively initiating and installing cloud-based applications.	K5
CO3	Explain how IOT can be used in different Industries.	K2
CO4	Identify how companies can plan for the future of technologies.	K3
CO5	Apply smart applications in real world.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Cloud Computing Fundamental-Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS, Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud

UNIT-II: Cloud Applications-Development environments for service development; Amazon, Azure, Google App, Security management in the cloud – security



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud

UNIT-III: The Internet of Things-An Overview of Internet of things, Internet of Things Technology, behind IoTs Sources of the IoTs, M2M Communication, Examples OF IoTs, Design Principles For Connected Devices Internet Connectivity Principles, Internet connectivity, Application Layer Protocols: HTTP, HTTPS, FTP, Telnet

UNIT-IV: IOT Design-Business Models for Business Processes in the Internet of Things, IoT/M2M systems LAYERS AND designs standardizations ,Modified OSI Stack for the IoT/M2M Systems, ETSI M2M domains and High-level capabilities ,Communication Technologies, Data Enrichment and Consolidation and Device Management Gateway Ease of designing and affordability

UNIT-V: IOT Security Issues- Secure constrained devices, Authorize and authenticate devices, Manage device updates, secure communication, Ensure data privacy and integrity, secure web, mobile, and cloud applications, Ensure high availability, Detect vulnerabilities and incidents, Manage vulnerabilities, Predict and preempt security issues.

Text Books:

1. Internet of Things: Architecture, Design Principles And Applications, 1st Edition, Rajkamal, McGraw Hill Higher Education, 2017
2. Internet of Things, 1st ed, A.Bahgya and V.Madisetti, University Press, 2015

Reference Books:

1. Enterprise Cloud Computing Technology Architecture Applications, 1st Edition, Gautam Shroff, Cambridge University Press, 2010
2. Cloud Computing, A Practical Approach, 1st Edition, Toby Velte, Anthony Velte, Robert Elsen peter, McGraw Hill, 2010
3. IOT Security Issues, 1st Edition, Alasdair Gilchrist, O'Reilly Publishers, 2017
4. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, 1st Edition, Tim Mather, Subra Kumara swamy, Shahed Latif, O'Reilly Publication, 2009

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	ML Applications to Security (R23MCY1153)	L	T	P	C
		3	0	0	3

Course Objectives: The main objective of this course is to Introduce cyber systems in different domains with the objective of securing cyber systems using machine learning

Course Outcomes:

Upon successful completion of this course, students will be able to:

- Apply the concepts of machine learning to secure cyber systems

Course Outcomes		Knowledge Level (K)#
CO1	Analyze the key features (aspects) to extract from Machine Learning from a security perspective.	K4
CO2	Assessing various classification and clustering mechanisms	K5
CO3	Explain the mechanisms of anomaly detection and intrusion detection and Challenges of Using Machine Learning in Anomaly Detection	K2
CO4	Identify how machine learning algorithms assist in planning to handle malware and network traffic analysis .	K3
CO5	Apply ML applications in protecting consumer web.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT I:

Machine Learning and Security: Cyber Threat Landscape, The Cyber Attacker's Economy, A Marketplace for Hacking Skills, Indirect Monetization, Machine Learning, Adversaries Using Machine Learning, Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach, Limitations of Machine Learning in Security

Machine Learning: Problems and Approaches, Machine Learning in Practice: A Worked Example, Training Algorithms to Learn, Model Families, Loss Functions, Optimization



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT II:

Classifying and Clustering:

Supervised Classification Algorithms, Logistic Regression, Decision Trees, Decision Forests, Support Vector Machines, Naive Bayes, k-Nearest Neighbors, Neural Networks, Practical Considerations in Classification, Selecting a Model Family, Training Data Construction, Feature Selection, Overfitting and Underfitting, Choosing Thresholds and Comparing Models

Clustering: Clustering Algorithms, Evaluating Clustering Results

UNIT III:

Anomaly Detection: Using Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection,

Host Intrusion Detection, Network Intrusion Detection, Web Application Intrusion Detection, Anomaly Detection with Data and Algorithms, Forecasting (Supervised Machine Learning), Statistical Metrics, Goodness-of-Fit, Unsupervised Machine Learning Algorithms, Density-Based Methods, Challenges of Using Machine Learning in Anomaly Detection, Response and Mitigation, Practical System Design Concerns, Optimizing for Explainability, Maintainability of Anomaly Detection Systems, Integrating Human Feedback, Mitigating Adversarial Effects

UNIT IV:

Malware Analysis: Understanding Malware, Defining Malware Classification, Malware: Behind the Scenes, Feature Generation, Data Collection, Generating Features, Feature Selection, From Features to Classification, Getting Malware Samples and Labels

Network Traffic Analysis: Theory of Network Defense, Access Control and Authentication, Intrusion Detection, Detecting In-Network Attackers, Data-Centric Security, Honeypots

Machine Learning and Network Security: From Captures to Features, Threats in the Network, Botnets and You, Building a Predictive Model to Classify Network Attacks, Exploring the Data, Data Preparation, Classification, Supervised Learning, Semi-Supervised Learning, Unsupervised Learning, Advanced Ensembling

UNIT V:

Protecting the Consumer Web: Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them, Supervised Learning for Abuse Problems, Clustering Abuse Production Systems: Defining Machine Learning System Maturity and Scalability, Data Quality, Model Quality, Performance, Maintainability, Monitoring and Alerting, Security and Reliability

Adversarial Machine Learning: The Importance of Adversarial ML, Security Vulnerabilities in Machine Learning Algorithms, Attack Technique: Model Poisoning, Attack Technique: Evasion Attack.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Text Books:

1. "Machine Learning and Security: Protecting Systems with Data and Algorithms" by Clarence Chio and David Freeman
2. "Machine Learning and Data Mining for Computer Security: Methods and Applications" by Marcus A. Maloof, Springer, 2006

Reference Books:

1. "Data Science for Cyber Physical Systems" by Sridhar Chimalakonda, Surya Nepal, and Raj Gaire

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Networks Security (R23MCY1154)	L	T	P	C
		3	0	0	3

Course Objectives: This course equips the system Administrators with the skills required to protect & recover the computer systems & networks from various security threats.

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

Course Outcomes		Knowledge Level (K)#
CO1	Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks.	K2
CO2	Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks	K3
CO3	Have a broad knowledge of the state-of-the-art and open problems in wireless and mobile security, thus enhancing their potential to do research or pursue a career in this rapidly developing area.	K4
CO4	Learn various security issues involved in cloud computing.	K5
CO5	Learn various security issues related to GPRS and 3G	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I:

Security Issues in Mobile Communication: Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – level Security.

UNIT-II:



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attack Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT-III:

Application Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications, GPRS Security for applications, UMTS security for applications, 3G security for applications, Some of Security and authentication Solutions

UNIT-IV:

Application Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions.

Ubiquitous Computing(UC), Need for Novel Security Schemes for UC, Security Challenges for UC, and Security Attacks on UC networks, Some of the security solutions for UC.

UNIT-V:

Data Center Operations - Security challenge, implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards

Text Books:

1. Pallapa Venkataram, Satish Babu: "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill, 2010.
2. Frank Adelstein, K.S.Gupta : "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.

Reference Books:

1. Randall k. Nichols, Panos C. Lekkas : "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
2. Bruce Potter and Bob Fleck : "802.11 Security" , 1st Edition, SPD O'REILLY 2005.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

3. James Kempf: “Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols”, 1st Edition, Cambridge University Press, 2008.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Cyber Security Operations and Design (R23MCY1154)	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand the concept of full-spectrum cyberspace operations, the complexities of the cyberspace environment, as well as planning, organizing, and integrating cyberspace operations.
- Students will have a fundamental understanding of how to analyze, plan for, and execute cyberspace operations.
- To learn and understand Cyber Warriors and Warrior Corps.

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

Course Outcomes		Knowledge Level (K)#
CO1	Explain the Concept of Cyberspace Environment and Design.	K2
CO2	Explain the Cyberspace Operational Approaches.	K2
CO3	Outline the cyberspace operation and integrate it with a Joint Operations plan.	K2
CO4	Build Cyber Warriors and Warrior Corps	K3
CO5	Designing Cyber Related Commands and Organizational structures.	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Understanding the Cyberspace Environment and Design- Cyberspace environment and its characteristics, developing a design approach, planning for cyberspace operation

UNIT-II: Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, the pros and cons of the



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

different approaches, Cyberspace Operations- Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defence and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations

UNIT-III: Cyberspace Integration- Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application Experiment

UNIT-IV: Building Cyber Warriors and Warrior Corps- The warrior and warrior corps concept as applied to cyber organizations, the challenges of training and developing a cyber-workforce from senior leadership to the technical workforce

UNIT-V: Designing Cyber Related Commands- Mission statements, Essential tasks, Organizational structures, Tables of organizations, Training and Readiness for Cyber Related Commands- Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization

Text Books:

1. Introduction of Cyber Warfare: A Multidisciplinary Approach, 1st Edition, Paulo Shakarian et al., syngress, Elsevier 2013
2. Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Edition, Jeffery carr et al, O'Reilly Publication December 2012

Reference Books:

1. Cyber Warfare: Techniques, 2nd Edition, Tactics and Tools for Security Practitioners Syngress, Jason Andress et al., Elsevier 2013

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Database and Web Applications Security (R23MCY1154)	L 3	T 0	P 0	C 3
----------------------------	--	----------------------	----------------------	----------------------	----------------------

Course Objectives:

- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To design security applications in the field of Information technology.
- To understand the fundamentals of database design, DB security and SQL extensions to security.
- To learn the basic concepts of Penetration testing.

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

Course Outcomes		Knowledge Level (K)#
CO1	Explain threats, vulnerabilities and breaches to design database	K2
CO2	Discuss Relational Data Model and concurrency controls and locking, SQL extensions to security.	K6
CO3	Demonstrate the Browser security principles.	K2
CO4	Analyze the software centric security and mobile web browser security in real time applications	K4
CO5	Construct the penetrating testing workflows with examples.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Database security-Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security, concepts, approaches and challenges, types of access controls, Oracle VPD, Discretionary and Mandatory access control: Principles, applications and poly instantiation, Database inference problem, types of inference attacks, distributed database, security levels, SQL-injection: types and advanced concepts



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-II: Relational Data Model- Security in relational data model, concurrency controls and locking, SQL extensions to security (oracle as an example), System R concepts, Context and control based access control, Hippocratic databases, Database watermarking, Database intrusion, Secure data outsourcing.

UNIT-III: Web application security-Basic principles and concepts, Authentication, Authorization, Browser security principles; XSS and CSRF, same origin policies, File security principles, Secure development and deployment methodologies, Web DB principles, OWASP – Top 10 -Detailed treatment, IoT security.

UNIT-IV: Mobile device security: Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security, Application security: Concepts, CIA Triad, Hexad, types of cyber-attacks, Introduction to software development vulnerabilities, code analyzers – Static and dynamic analyzers.

UNIT-V: Penetration testing- Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates.

Text Books:

1. Web Application Security, 1st Edition, A Beginners Guide, Bryan and Vincent, McGraw-Hill, 2011
2. Database Security, 1st Edition, Alfred Basta, Melissa Zgola, Course Technology, 2012

Reference Books:

1. Handbook of Database Security: Applications and Trends, Michael Gertz and Sushil Jajodia, Springer, 2008
2. Database and Applications Security, 1st Edition, Integrating Information Security and Data Management, Bhavani Thuraisingham, Auerbach Publications, 2005

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Block Chain Technologies (R23MCY1154)	L	T	P	C
		3	0	0	3

Course Objectives:

1. To learn the fundamentals of Block Chain and various types of block chain and consensus mechanism.
2. To understand public block chain system, Private block chain system and consortium block chain.
3. Able to know the security issues of blockchain technology.

Course Outcomes:

1. Able to work in the field of block chain technologies.

UNIT – I:

Fundamentals of Blockchain: Introduction, Origin of Blockchain, Blockchain Solution, Components of Blockchain, Block in a Blockchain, The Technology and the Future.

Blockchain Types and Consensus Mechanism: Introduction, Decentralization and Distribution, Types of Blockchain, Consensus Protocol.

Cryptocurrency: Bitcoin, Altcoin and Token: Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics, Types of Cryptocurrencies, Cryptocurrency Usage.

UNIT – II:

Public Blockchain System: Introduction, Public Blockchain, Popular Public Blockchains, The Bitcoin Blockchain, Ethereum Blockchain.

Smart Contracts: Introduction, Smart Contract, Characteristics of a Smart Contract, Types of Smart Contracts, Types of Oracles, Smart Contracts in Ethereum, Smart Contracts in Industry.

UNIT – III:

Private Blockchain System: Introduction, Key Characteristics of Private Blockchain, Private Blockchain, Private Blockchain Examples, Private Blockchain and Open Source, E-commerce Site Example, Various Commands (Instructions) in E-commerce Blockchain, Smart Contract in Private Environment, State Machine, Different Algorithms of Permissioned Blockchain, Byzantine Fault, Multichain.

Consortium Blockchain: Introduction, Key Characteristics of Consortium Blockchain, Need of Consortium Blockchain, Hyperledger Platform, Overview of Ripple, Overview of Corda.

Initial Coin Offering: Introduction, Blockchain Fundraising Methods, Launching an ICO, Investing in an ICO, Pros and Cons of Initial Coin Offering, Successful Initial Coin Offerings, Evolution of ICO, ICO Platforms.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT – IV:

Security in Blockchain: Introduction, Security Aspects in Bitcoin, Security and Privacy Challenges of Blockchain in General, Performance and Scalability, Identity Management and Authentication, Regulatory Compliance and Assurance, Safeguarding Blockchain Smart Contract (DApp), Security Aspects in Hyperledger Fabric.

Applications of Blockchain: Introduction, Blockchain in Banking and Finance, Blockchain in Education, Blockchain in Energy, Blockchain in Healthcare, Blockchain in Real-estate, Blockchain in Supply Chain, The Blockchain and IoT. Limitations and Challenges of Blockchain.

UNIT – V:

Blockchain Case Studies:

Case Study 1 – Retail,

Case Study 2 – Banking and Financial Services,

Case Study 3 – Healthcare,

Case Study 4 – Energy and Utilities.

Blockchain Platform using Python: Introduction, Learn How to Use Python Online Editor, Basic Programming Using Python, Python Packages for Blockchain.

Blockchain platform using Hyperledger Fabric: Introduction, Components of Hyperledger Fabric Network, Chain codes from Developer.ibm.com, Blockchain Application Using Fabric Java SDK.

Text book:

1. “Block chain Technology”, Chandramouli Subramanian, Asha A.George, Abhilasj K A and Meena Karthikeyan , Universities Press.

Reference Books:

1. Blockchain Blue print for Economy, Melanie Swan, SPD Oreilly.
2. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gauar, Pearson Addition Wesley

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Research Methodology and IPR (R23MCY1155)	L	T	P	C
		2	0	0	2

Course Objectives:

- Student able analyze the Effective literature studies approaches, analysis, Plagiarism, Research ethics.
- Student should able understand problem, Scope and objectives of research problem.
- To learn and understand Traditional knowledge Case Studies, IPR and IITs

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

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the research and its types, Reviewing literature. Identifying and defining research problem.	K2
CO2	Explaining research design methods, sampling techniques	K5
CO3	Designing and development of measuring instruments, data collection and analysis methods	K6
CO4	Show the IPR protection provides an incentive to inventors for further research work and Investment in R & D, which leads to creation of new and better products, and in turn brings about, Economic growth and social benefits.	K1
CO5	Identify Research proposal, research report and evaluating research	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem, Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-II: Effective literature studies approaches, analysis, Plagiarism, Research ethics, Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

UNIT-III: Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT

UNIT-IV: Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications

UNIT-V: New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

Text Book:

1. Research methodology: an introduction for science & engineering students, 1st Edition, [Stuart Melville](#), [Wayne Goddard](#), 1996

Reference Books:

1. Research Methodology: A Step by Step Guide for beginners, 2nd Edition, Ranjit Kumar, 2011
2. Resisting Intellectual Property, 1st Edition, Halbert, Taylor & Francis Ltd., 2007

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Cryptography Lab (R23MCY1156)	L	T	P	C
		0	0	3	1.5

Course Objectives:

1. Explain the objectives of information security.
2. Explain the importance and application of each of confidentiality, integrity, authentication and availability.
3. Understand various cryptographic algorithms.

Course Outcomes:

1. Understand basic cryptographic algorithms, message and web authentication and security issues.
2. Identify information system requirements for both of them such as client and server.
3. Understand the current legal issues towards information security.

List of Experiments:

1. Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should XOR each character in this string with 0 and displays the result.
2. Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should AND or and XOR each character in this string with 127 and display the result.
3. Write a Java program to perform encryption and decryption using the following algorithms a. Ceaser cipher b. Substitution cipher c. Hill Cipher
4. Write a C/JAVA program to implement the DES algorithm logic.
5. Write a C/JAVA program to implement the Blowfish algorithm logic.
6. Write a C/JAVA program to implement the Rijndael algorithm logic.
7. Write the RC4 logic in Java Using Java cryptography; encrypt the text "Hello world" using Blowfish. Create your own key using Java key tool.
8. Write a Java program to implement RSA algorithm.
9. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.
10. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.
11. Calculate the message digest of a text using the MD5 algorithm in JAVA.

Text Books:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition.
2. Cryptography and Network Security: Atul Kahate, McGraw Hill, 3rd Edition.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Reference Books:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, McGraw Hill, 3rd Edition.
3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH.
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning.
6. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	English for Research Paper Writing (R23MCY1157)	L	T	P	C
		2	0	0	0

Course Objectives:

- Understand that how to improve your writing skills and level of Readability
- Learn about what to write in each section
- Understand the skills needed when writing a Title

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

Course Outcomes		Knowledge Level (K)#
CO1	How to improve your writing skills and level of readability	K1
CO2	Explain about what to write in each section	K3
CO3	Classify the skills needed when writing a Title	K2

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness

UNIT-II: Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts Introduction

UNIT-III: Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.

UNIT-IV: Key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-V: Skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions

UNIT-VI: Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission.

Text Books:

1. Writing for Science, 0th Edition, Yale University Press, Goldbort R 2006
2. How to Write and Publish a Scientific Paper, 7th Edition, Cambridge University Press, Day R 2006
3. Handbook of Writing for the Mathematical Sciences, 2nd Edition, SIAM, Highman's book, Highman N 1998

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Disaster Management (R23MCY1157)	L	T	P	C
		2	0	0	0

Course Objectives:

- Learn to demonstrate a critical understanding of key concepts in disaster risk reduction and humanitarian response.
- Critically evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.
- Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.
- critically understand the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in

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

Course Outcomes		Knowledge Level (K)#
C01	Demonstrate the critical understanding of key concepts in disaster risk reduction and humanitarian response.	K2
C02	Evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.	K5
C03	Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.	K6
C04	Analyze the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in	K4
C05	Describe disaster risk reduction and humanitarian response. Outline the disaster risk reduction and humanitarian response policy and practice from multiple perspectives.	K2,K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-I: Introduction- Disaster- Definition, Factors and Significance; Difference between Hazard and Disaster; Natural and Manmade Disasters: Difference, Nature, Types and Magnitude.

UNIT-II: Repercussions of Disasters And Hazards- Economic Damage, Loss of Human and Animal Life, Destruction of Ecosystem. Natural Disasters- Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts and Famines, Landslides and Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks and Spills, Outbreaks of Disease and Epidemics, War and Conflicts.

UNIT-III: Disaster Prone Areas In India- Study of Seismic Zones; Areas Prone to Floods and Droughts, Landslides and Avalanches, Areas Prone to Cyclonic and Coastal Hazards With Special Reference to Tsunami, Post-Disaster Diseases and Epidemics

UNIT-IV: Disaster Preparedness And Management- Preparedness: Monitoring of Phenomena Triggering A Disaster or Hazard; Evaluation of Risk: Application of Remote Sensing, Data from Meteorological and other Agencies, Media Reports: Governmental and Community Preparedness.

UNIT-V: Risk Assessment- Disaster Risk: Concept and Elements, Disaster Risk Reduction, Global and National Disaster Risk Situation. Techniques of Risk Assessment, Global Co-Operation in Risk Assessment and Warning, People's Participation in Risk Assessment, Strategies for Survival.

Disaster Mitigation- Meaning, Concept and Strategies of Disaster Mitigation, Emerging Trends in Mitigation, Structural Mitigation and Non-Structural Mitigation, Programs of Disaster Mitigation In India.

Text Books:

1. Disaster Management in India: Perspectives, issues and strategies, R. Nishith, Singh AK, New Royal book Company
2. Disaster Mitigation Experiences and Reflections, Sahni, New Title Edition , Pardeep Et. Al. (Eds.), Prentice Hall Of India, New Delhi
3. Disaster Administration and Management Text and Case Studies, 1st Edition, Deep & Deep Publication Pvt. Ltd., Goel S. L., New Delhi

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Sanskrit for Technical Knowledge (R23MCY1157)	L	T	P	C
		2	0	0	0

Course Objectives:

- To get a working knowledge in illustrious Sanskrit, the scientific language in the world
- Learning of Sanskrit to improve brain functioning
- Learning of Sanskrit to develop the logic in mathematics, science & other subjects
- enhancing the memory power
- The engineering scholars equipped with Sanskrit will be able to explore the
- Huge knowledge from ancient literature

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

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate basic Sanskrit language	K2
CO2	Illustrate Ancient Sanskrit literature about science & technology	K2
CO3	Build a logical language will help to develop logic in students	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Alphabets in Sanskrit, Past/Present/Future Tense.

UNIT-II: Simple Sentences forming in Sanskrit.

UNIT-III: Order of Sanskrit sentences, Introduction of roots in Sanskrit language.

UNIT-IV: Technical information about Sanskrit Literature.

UNIT-V: Technical concepts of Engineering-Electrical, Mechanical, Architecture, Mathematics.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Text Books:

1. Abhyaspustakam – Dr.Vishwas, 1st Edition, Samskrita-Bharti Publication, New Delhi
2. Teach Yourself Sanskrit, Prathama Deeksha, VempatiKutumbshastri, Rashtriya Sanskrit Sansthanam, New Delhi Publication
3. India's Glorious Scientific Tradition, 1st Edition, Suresh Soni, Ocean books (P) Ltd., New Delhi

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - I Semester	Value Education (R23MCY1157)	L	T	P	C
		2	0	0	0

Course Objectives:

- Understand value of education and self- development
- Imbibe good values in students
- Let the should know about the importance of character

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

Course Outcomes		Knowledge Level (K)#
CO1	Infer the knowledge of self-development	K2
CO2	Describe the importance of Human values	K2
CO3	Developing the overall personality	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Values and self-development- Social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non- moral valuation, Standards and principles, Value judgments

UNIT-II: Importance of cultivation of values- Sense of duty, Devotion, Self-reliance, Confidence, Concentration. Truthfulness, Cleanliness, Honesty, Humanity, Power of faith, National Unity, Patriotism. Love for nature, Discipline.

UNIT-III: Personality and Behaviour Development-Soul and Scientific attitude, Positive Thinking, Integrity and discipline, Punctuality, Love and Kindness, Avoid fault Thinking.

UNIT – IV: Free from anger, Dignity of labour- Universal brotherhood and religious tolerance, True friendship, Happiness Vs suffering, love for truth, Aware of self-destructive habits, Association and Cooperation, Doing best for saving nature.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT – V: Character and Competence- Holy books vs Blind faith, Self-management and Good health, Science of reincarnation, Equality, Nonviolence, Humility, Role of Women, All religions and same message, Mind your Mind, Self-control, Honesty, Studying effectively.

Text Books:

1. Values and Ethics for organizations Theory and practice, Latest Edition, Chakroborty, S.K., Oxford University Press, New Delhi

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Cyber Crime Investigation and Digital Forensics (R23MCY1251)	L	T	P	C
		3	0	3	4.5

Course Objectives:

- Able to identify security risks and take preventive steps
- To understand the forensics fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of digital evidence.

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

	Course Outcomes	Knowledge Level (K)#
C01	Explain the computer forensics fundamentals.	K2
C02	Describe the types of computer forensics technology	K3
C03	Analyze various computer forensics systems.	K4
C04	Illustrate the methods for data recovery, evidence collection and data seizure.	K2
C05	Identify the Role of CERT-In Security	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction- Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT-II: Cyber Crime Issues- Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-III: Investigation- Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT-IV: Digital Forensics- Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

UNIT-V: Role of CRET-In Cyber Security- Computer Security Incident Response (Reactive) – Computer Security Incident Prevention (Proactive) – Security Quality Management Services, CERT-In Security Guidelines- Web server, database server, Intrusion Detection system, Routers, Standard alone system, networked System, IT Security polices for government and critical sector organizations.

List of Experiments:

Experiment- 1

Evidence Collection

a) Linux: Capturing RAM dump using fmem

<https://github.com/NateBrune/fmem>

i) dcfldd if=/dev/fmem of=memory.dump hash=sha256
sha256log=memory.dump.sha256 bs=1MB count=1000

b) Linux: Capturing Disk using dfldd

<https://www.obsidianforensics.com/blog/imaging-using-dcfldd>

i) dcfldd if=/dev/sdb1 of=/media/disk/test_image.dd hash=md5,
sha1hashlog=/media/disk/hashlog.txt

Experiment- 2

a) Windows: Capture RAM dump of a windows system

a. Hint: FTK Imager or RAM Capture

b) Windows: Capture Disk Image of a windows system

Hint: FTK Imager

Experiment- 3

Disk Analysis

i) List all files in a directory from a disk image

a. FTK Imager



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

- ii) Export a particular file from a disk image
 - a. FTK Imager
- iii) Recover a deleted file from a disk image

Hint: FTK Imager

Experiment- 4

Memory Analysis

- 1. List all running processes from a memory image
- 2. List all network connections from a memory image
- 3. Find out whether a firewall is set by analyzing a memory image

Hint: volatility

Experiment- 5

Live Incident Response

- 1. Perform live incident response on a system
- 2. View all browser history in a computer
- 3. List out all established network connections in a computer

Hint: Triage Incident Response

Experiment – 6: Implement E-Mail Tracking and Email Investigation

Experiment – 7: Implement video Analytics for a live video

Experiment – 8: Analysis on different Malware Working

Experiment - 9: Work on Mail Bombs &SMS bombs

Experiment – 10: Implement a case on windows and Linux forensics

Experiment – 11: Implement a case on network Forensic

Experiment – 12: Work on different types of vulnerabilities

Experiment-13: Implement a case on Mobile Forensics

Experiment -14: Develop a Evidence and Preparation and Documentation

Experiment -15: Using kgbkeylogger tool record or generate a document what a user working on system



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Textbook:

1. Digital Forensics Basics: A Practical Guide Using Windows OS Paperback, 1st Edition, February 26, 2019

Reference Books:

1. Computer Forensics and Investigations, Nelsonm Phillips and Enfinger Steuart, 5th Edition, Cengage Learning, New Delhi, 2009
2. Incident Response and Computer Forensics, Kevin Mandia, Chris Prosise, Matt Pepe, 1st Edition, Tata McGraw-Hill, New Delhi, 2006
3. Software Forensics, Robert M Slade, Tata McGraw - Hill, New Delhi, 2005

Web Reference:

1. CERT-In Guidelines-<http://www.cert-in.org.in/>

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Web Security (R23MCY1252)	L	T	P	C
		3	0	0	3

Course Objectives:

- Underlying security principles of the web
- Overview of concrete threats against web applications
- Insights into common attacks and countermeasures
- Current best practices for secure web applications

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

	Course Outcomes	Knowledge Level (K)#
CO1	Demonstrate security concepts, security professional roles, and security resources in the context of systems and security development life cycle	K2
CO2	Justify applicable laws, legal issues and ethical issues regarding computer crime	K5
CO3	Explain the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development	K2
CO4	Apply information security policies, standards and practices, the information security blueprint	K3
CO5	Analyze and describe security requirements for typical web application scenario	K4

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-I: Introduction-A web security forensic lesson, Web languages, Introduction to different web attacks, Overview of N-tier web applications, Web Servers-Apache, IIS.

UNIT-II: Securing the Communication Channel- Understanding the dangers of an insecure communication channel. Practical advice on deploying HTTPS, and dealing with the impact on your application, Insights into the latest evolutions for HTTPS deployments.

UNIT-III: Web Hacking Basics- HTTP & HTTPS URL, Web under the Cover Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS.

UNIT-IV: Securely Handling Untrusted Data-Investigation of injection attacks over time, Understanding the cause behind both server-side and client-side injection attacks, Execution of common injection attacks, and implementation of various defenses.

UNIT-V: Preventing Unauthorized Access-Understanding the interplay between authentication, authorization and session management. Practical ways to secure the authentication process prevent authorization bypasses and harden session management mechanisms, Securing Large Applications, Cyber Graffiti.

Text Books:

1. Web Hacking: Attacks and Defense, Latest Edition , McClure, Stuart, Saumil Shah, and Shreeraj Shah, Addison Wesley, 2003
2. Professional Java Security, 1.3 Edition, Garms, Jess and Daniel Somerfield, Wrox, 2001

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Software Vulnerability Analysis (R23MCY1253)	L	T	P	C
		3	0	0	3

Course Objectives:

- This course provides the user to know the software vulnerabilities in the real software world.
- Different application level security
- Able to find the malicious code actions and different protection techniques.

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

	Course Outcomes	Knowledge Level (K)#
CO1	Contrast the basic concepts of security & Authentication	K2
CO2	Illustrate the Malicious Code in software applications	K2
CO3	Analyze and apply Access Control & Physical Protection to the UNIX and Windows operating system	K4
CO4	Explain the concepts of OSI Model, Sockets	K2
CO5	Explain the concepts of Counter Measures	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction to security & Authentication- Software Security Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest, Technical Trends Affecting Software Security, The ileitis, Beyond Reliability, Penetrate and Patch, On Art and Engineering, Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality, Multilevel Security.

UNIT-II: Application Security & Malicious Code-Managing Software Security Risk: An Overview Of Software Risk Management For Security, The Role Of Security Personnel, Software Security Personnel In The Life Cycle, Deriving Requirements, Risk Assessment, Software Risk Management, Architectural Risk Analysis, Risk-Based Security Testing, Security Requirements, Security Operations.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-III: Access Control & Physical Protection- The UNIX Access Control Model, How UNIX and Windows Exploits, Modifying File Attributes, Modifying Ownership, The unmask, The Programmatic Interface, Setuid Programming, Access Control In Windows NT, Compartmentalization, Fine-Grained Privileges. Buffer Overflow & Root kits: Buffer Overflows As Security Problems, Defending Against Buffer Overflow.

UNIT-IV: Network Security& Intrusion- OSI Model, Sockets-Functions, Addresses, Network Byte Order, Internet Address Conversion, Simple Server and Web Clients, Tiny web Server. Peeling Back the Lower Layers, Network Sniffing, Raw Socket Sniffer, libpcap Sniffer, Decoding the Layers, Active Sniffing, Denial of Service, SYN Flooding, The Ping of Death, Teardrop, Ping Flooding, Amplification Attacks, Distributed DoS Flooding.

UNIT-V: Counter Measures- Detection of System Daemons, Crash Course in Signals, Tiny web Daemon, Tools of the Trade, tiny web Exploit Tool, Log Files, Log less Exploitation, Socket Reuse, Payload Smuggling, String Encoding, Buffer Restrictions, Polymorphic Printable ASCII Shell code. Hardening Countermeasures, Non executable Stack, ret2libc, Returning into system() Randomized Stack Space, Investigations with BASH and GDB, Bouncing Off Linux gate. Applied Knowledge, First Attempts, Paying the Odds.

Text Books:

1. Building Secure Software: How to Avoid Security Problems the Right Way, John Viega & Gary McGraw, Addison-Wesley Professional Computing Series, 1st Edition, 2019
2. Software Security: Building Security In, Gary McGraw, Addison-Wesley Professional Computing Series, 2006

Reference Books:

1. 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (Security One-off), Michael Howard, David LeBlanc, John Viega, Addison-Wesley Professional Computing Series, 2005
2. Hacking: The Art of Exploitation, 2nd Edition, Jon Erickson, No Starch Press, San Fransico, 2008
3. Software Security, Theory Programming and Practice, Richard Sinn, Cengage Learning, 2015

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Malware Analysis and Reverse Engineering (R23MCY1253)	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand the purpose of computer infection program.
- To implement the covert channel and mechanisms.
- To test and exploit various malware in open source environment.
- To analyze and design the famous virus and worms.
- Understand the Reverse Engineering (RE) Methodology
- Disassemble products and specify the interactions between its subsystems and their functionality

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

	Course Outcomes	Knowledge Level (K)#
C01	Explain the characteristics of Malware and its effects on Computing systems.	K2
C02	Predict the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.	K6
C03	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	K4
C04	Demonstrate the Malware functionalities.	K2
C05	Apply anti-reverse engineering in different Applications.	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-I: Malware Basics-Fundamentals of Malware Analysis (MA), MA tools and techniques, Static Malware Analysis, Dynamic Malware Analysis, Recent Malware Case Studies.

UNIT-II: Basic Analysis-Antivirus Scanning, x86 Disassembly, Hashing, Finding Strings, Packed Malware, PE File Format, Linked Libraries & Functions, PE Header File &Section.

UNIT-III: Advanced Static & Dynamic Analysis-IDA Pro, Recognizing C code constructs, Analyzing malicious windows program, Debugging, OllyDbg, Kernel Debugging with WinDbg, Malware Focused Network Signatures.

UNIT-IV: Malware Functionalities- Malware Behavior, Covert Malware Launch, Data Encoding, Shell code Analysis.

UNIT-V: Reverse Engineering Malware (REM)- REM Methodology, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAV Signatures, Creating Custom ClamAV Databases

Text books:

1. Computer Viruses: from theory to applications, Erci Filiol, 1st edition, Springer, 2005

Reference Books:

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski, Andrew Honig, publisher William Pollock, 2012

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Application Threat Detection (R23MCY1253)	L	T	P	C
		3	0	0	3

Course Objectives:

- Can detect threats to any web app.
- Able to perform various Input Injection Attacks.
- Able to provide countermeasures against various input injection attacks.

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

Course Outcomes		Knowledge Level (K)#
C01	Explain Hacking Web Apps and Profiling	K5
C02	Illustrate to provide Authentication to the web application.	K2
C03	Develop Penetration Testing and implement Input Injection Attacks.	K3
C04	Identify the basic fundamentals of Metasploit	K3
C05	Apply knowledge on Capturing User Input and Abusing UI Expectations	K3

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Hacking Web Apps and Profiling-Web Application Hacking: GUI web Hacking, URI Hacking, Methods Headers and Body, Resources, The Web Client and HTML, Other Protocols, How & Why Web Apps attack, Infrastructure Profiling: Foot printing and Scanning, Basic Banner Grabbing, Advanced HTTP Fingerprinting, Infrastructure Intermediaries. Application Profiling: Manual Inspection, Search Tools for Profiling, Automated Web Crawling, General Countermeasures.

UNIT-II: Bypassing and Attacking Web Authentication-Web Authentication Threats: Username/password Threats, Password Guessing and its Countermeasures,

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Eavesdropping attacks and its Countermeasures, Forms-based Authentication attacks and its countermeasures. Stronger web Authentication, Web Authentication Services. Bypassing Authentication: Token Replay, Cross-site Request Forgery, and Identity Management.

UNIT-III: Penetration Testing and Input Injection Attacks- Where to find Attack vectors, Common Input Injection Attacks: Buffer Overflow, Canonicalization and its countermeasures, Advanced Directory Traversal, Navigating Without Directory Listing, HTML Injection: XSS, Embedded scripts, Cookies and Predefined Headers, Counter countermeasures. SQL Injection: SUB Queries, UNION, SQL Injection countermeasures, XPATH Injection and its countermeasures, LDAP Injection.

UNIT-IV: Metasploit-Basics of Penetration Testing: The Phase of PTES, Types of Penetration Tests. Metasploit: Introduction, Metasploit Basics: Terminology, Metasploit Interfaces, Metasploit Utilities. Intelligence Gathering: Passive Information Gathering, Active Information Gathering, Target Scanning. Vulnerability Scanning: Basic Vulnerability Scan, Scanning with scanning tools, Using Scan Results for Autopwning.

UNIT-V: Attacking Users-Defacing Content, Capturing User Input: Using Focus Event, Using Keyboard Events, Using Mouse and Pointer Events, Using Form Events, Social Engineering: Using TabNabbing, Abusing UI Expectations: Using Fake Login Prompts, Pretty Theft, Gmail Phishing

Text Books:

1. Hacking Exposed Web Application, 3rd Edition by Joel Scambray, Vincent Liu, Caleb Sima, 2010
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition, Dafydd Stuttard, Marcus Pinto Wiley Publication, 2011
3. Metasploit - The Penetration Tester's Guide, 1st Edition, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni – No Starch Press Publication, 2011

Reference Books:

1. The Browser Hacker's Handbook by Wade Alcorn, 1st Edition, Christian Frichot and Michele Orru, Wiley Publication, 2014
- Web Penetration Testing with Kali Linux, 3rd Edition, Joseph Muniz, AamirLakhan, Packt Publication, 2013

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Information System Audit (R23MCY1253)	L	T	P	C
		3	0	0	3

Course Objectives:

- Understanding and knowledge of Security Auditing, and introduce the Threats and defense in the systems.
- Acquiring the knowledge on Evidence collection and evaluation techniques.

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

	Course Outcomes	Knowledge Level (K)#
CO1	Illustrate the fundamental concepts of information security and systems auditing	K2
CO2	Analyze the latest trend of computer security threats and defense	K4
CO3	Identify security weaknesses in information systems, and rectify them with appropriate security mechanisms	K3
CO4	Explain the security controls in the aspects of physical, logical and operational security control and case studies	K5
CO5	Evaluate the security of information systems	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Overview of Information System Auditing- Effect of Computers on Internal Controls, Effects of Computers on Auditing, Foundations of information Systems Auditing, Conducting an Information Systems Audit.

UNIT-II: The management Control Framework-I- Introduction, Evaluating the planning Function, Leading Function, Controlling Function, Systems Development Management Controls, Approaches to Auditing Systems Development, Normative Models of the Systems Development Process, Evaluating the Major phases in the Systems Development Process, Programming Management Controls, Data Resource Management Controls.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-III: The Management Control Framework-II- Security Management Controls, Operations management Controls Quality assurance Management Controls, Case Studies.

UNIT-IV: Evidence Collection- Audit Software, Code Review, Test Data, and Code Comparison, Concurrent Auditing techniques, Interviews, Questionnaires, and Control Flowcharts. Performance Management tools- Case Studies.

UNIT-V: Evidence Evaluation- Evaluating Asset Safeguarding and Data Integrity, Evaluating System, Effectiveness, Evaluating System Efficiency, Information Systems Audit and Management: Managing the Information Systems Audit Function.

Reference Books:

1. Information Systems Control and Audit, 1st Edition, Ron Weber, Pearson Education, 2013
2. Information System Audit and Assurance, D P Dube, TMH, New Delhi, 2008

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Biometric Security (R23MCY1254)	L	T	P	C
		3	0	0	3

Course Objectives:

- Describe the principles of the three core biometric modalities (face, fingerprint and iris), and know how to deploy them in authentication scenarios
- Organize and conduct biometric data collections, and apply biometric databases in system evaluation
- Calculate distributions of within- and between-class matching scores, and calculate various error estimates based on these distributions
- Identify the privacy and security concerns surrounding biometric systems, and know how to address them in such a way that balances both
- Recognize differences between algorithm design and systems engineering in biometrics
- Deploy statistical methods in biometric system evaluation
- Itemize the most up-to-date examples of real biometric applications in human authentication.

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

	Course Outcomes	Knowledge Level (K)#
C01	Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems	K2
C02	Analyze biometric systems at the component level and be able to analyze and design basic biometric system applications	K4
C03	Illustrate to work effectively in teams and express their work and ideas orally and in writing	K2
C04	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems	K3
C05	Elaborate various Biometric security issues in real world applications	K6

#Based on suggested Revised BTL

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Biometrics- Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems

UNIT-II: Physiological Biometric Technologies- Fingerprints, Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment, Facial scan, Technical description, characteristics, weaknesses, deployment, Iris scan, Technical description, characteristics, strength, weaknesses, deployment

UNIT-III: Physiological Biometric Technologies- Hand Biometric: Palm Print, Vein Pattern, Signature and Hand Writing Technology-Technical description, characteristics, strengths, weaknesses and deployment.

UNIT-IV: Behavioural Biometric Technologies- Voice Recognition and Key stroke dynamics: Introduction, working, strengths and weaknesses, Voice Recognition Applications, Understanding Voice Recognition, Choice of Features, Speaker modeling, Pattern Matching, Key Stroke Dynamics, Active and Passive Biometrics.

UNIT – V: Multi biometrics and multi factor biometrics- two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan, Securing Biometric Template- Cancelable Biometrics, Authentication, Security Analysis.

Text Books:

1. A Privacy Enhancing Biometric, Chuck Wilson, Vein pattern recognition, CRC press, 1st Edition, 2010
2. Biometrics: Identity Verification in a Network, 1st Edition, Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Wiley Eastern, 2002
3. Implementing Biometric Security, 1st Edition, John Chirillo and Scott Blaul Wiley Eastern Publication, 2005

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	AI in Cyber Security (R23MCY1254)	L	T	P	C
		3	0	0	3

Course Objectives:

- Understand the role of artificial intelligence (AI) in the context of cyber security.
- Explore techniques and applications of AI in cyber threat detection and prevention.

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

	Course Outcomes	Knowledge Level (K)#
CO1	Explain fundamental concepts and the role of AI in cyber security.	K2
CO2	Apply AI techniques for cyber threat detection	K4
CO3	Analyze the threat modelling techniques.	K2
CO4	Apply AI Applications in Cyber Threat Analytics	K3
CO5	Demonstrate the application of AI in threat detection	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						
CO4						
CO5						

(Please fill the above with Levels of Correlation, viz., L, M, H)

Unit-I:

AI Role in Cybersecurity: Applying Artificial Intelligence in Incident Response: Analyzing potential Indicators and Determine the Type of Attack, Vulnerability Management and Prioritization, Security Governance and Policies, Create Secure network designs, Fraud Detection and Prevention, Cryptography, Identity and Access Management(IAM). (Text Book 1)

Unit-II:

Cyber Threat Intelligence with AI: Cyber Threat framework architecture and operating model, Lookheed Martin's cyber kill chain framework, integrating cyber kill chain model into an intelligence project, Benefits of the kill chain, MITRE ATT&CK



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

knowledge-based framework, Diamond model of intrusion analysis framework. (Text Book 2)

Unit- III:

Threat Modelling and Adversary Analysis: Threat Modelling process: Identifying and decomposing assets, Adversaries and threat analysis, Attack surfaces and threat vectors, Adversary analysis use case – twisted spider, system re-evaluation.
Adversary Analysis: Adversary attack preparation, countermeasures, attack simulation, execution, and mitigation procedures. (Text Book 2)

Unit- IV:

AI Applications in Cyber Threat Analytics: Adversaries leveraging AI, Cyber Threat Hunting, Integration Strategy, Threat Hunting Process, AI's position in the CTI program and security stack. AI Integration – the IBM Qradar Advisor approach. (Text Book 2)

Unit-V:

Detecting Threats with AI: Email Threats with AI(Detecting spam with perceptron, Spam detection with SVM's, Phishing detection with Naïve Bayes) Malware Threat Detection (Identifying malware families, Decision tree malware detectors, metamorphic malware with HMMs, Advanced malware Detection with Deep learning) (Text Book 3)

Textbooks:

1. The AI Revolution in Networking, Cybersecurity, and Emerging Technologies by Omar Santos, Samer Salam, HazimDahir, Feb 2024.
2. Mastering Cyber Intelligence by Jean Nestor M.Dahj, April 2022.
3. Hands-On Artificial Intelligence for Cybersecurity by Alessandro Parisi, Aug 2019.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Ethical Hacking (R23MCY1254)	L	T	P	C
		3	0	0	3

Course Objectives:

- The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
- The course includes-Impacts of Hacking; Types of Hackers; Information Security Models, Information Security Program, Business Perspective, Planning a Controlled Attack
- Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

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

	Course Outcomes	Knowledge Level (K)#
C01	Explain the concepts related to malware, hardware and software vulnerabilities and their causes	K2
C02	Determine the applicable laws, legal issues and ethical issues regarding computer crime.	K4
C03	Explain the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development.	K2
C04	Demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system	K2
C05	Evaluate security techniques used to protect system and user data	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction to Hacking- Important Terminologies, Types of Ethical Hacking, phases of Ethical Hacking, Categories of Penetration Testing.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-II: Phases of Ethical Hacking I- Information Gathering Techniques, Target Enumeration and Port Scanning Techniques, Vulnerability Assessment.

UNIT-III: Phases of Ethical Hacking II-Network Sniffing, Exploitation, Remote Exploitation, Client Exploitation, Web Exploitation.

UNIT-IV: System Hacking- Password cracking techniques- Key loggers, Escalating privileges, Hiding Files, Double Encoding, Steganography technologies and its Countermeasures. Active and passive sniffing ARP Poisoning, MAC Flooding, SQL Injection, Error based, Union-based, Time-based, Blind SQL, Out-of-band, Injection Prevention Techniques.

UNIT-V: Hacking- Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, Client Mis-association, Wireless Hacking Methodology, Wireless Traffic Analysis. DNS Security,

Text book:

1. Hacking: Be a Hacker with Ethics, 2nd Edition, Harsh Bothra, Khanna Publications, 2019
2. Ethical Hacking and Penetration Testing Guide, 1st Edition, Rafay Baloch, 2014

Reference Books:

1. Kali Linux Wireless Penetration Testing Beginner's Guide, Vivek Ramachandran, 1st Edition, Cameron Buchanan, Packt Publishing, 2015
2. SQL Injection Attacks and Defense, 1st Edition, Justin Clarke-Salt, Syngress Publication, 2012
3. Mastering Modern Web Penetration Testing, Prakhar Prasad, Packt Publishing, October 2016

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Risk Management (R23MCY1254)	L	T	P	C
		3	0	0	3

Course Objectives:

- Understand the fundamentals of risk management.
- Explore techniques for identifying, assessing, and mitigating risks.
- Introduce risk management frameworks and methodologies.
- Understand the role of technology and data in modern risk management.
- Explore real-world applications of risk management in different industries.

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

	Course Outcomes	Knowledge Level (K)#
C01	Explain fundamental concepts and the importance of risk management.	
C02	Apply techniques for identifying and assessing risks.	
C03	Develop and evaluate risk mitigation strategies.	
C04	Understand and implement popular risk management frameworks and methodologies.	
C05	Demonstrate the application of risk management in real-world scenarios.	

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

Unit I:

Introduction to Risk Management: Fundamentals of Risk Management, Importance and Challenges of Risk Management, Overview of Different Types of Risks (Financial, Operational, Strategic, etc.), Role of Risk Management in Organizational Decision Making

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

Unit II:

Risk Identification and Assessment Techniques: Techniques for Identifying Risks, Risk Assessment Methods and Models, Quantitative vs. Qualitative Risk Assessment, Case Studies and Examples in Risk Identification and Assessment

Unit III:

Risk Mitigation Strategies: Risk Mitigation Approaches and Strategies, Developing Risk Response Plans, Evaluating the Effectiveness of Risk Mitigation, Case Studies on Successful Risk Mitigation

Unit IV:

Risk Management Frameworks and Methodologies: Overview of Popular Risk Management Frameworks (ISO 31000, COSO ERM, etc.), Agile Risk Management Methodologies, Integrating Risk Management into Project Management, Advanced Risk Modelling and Simulation Techniques

Unit V:

Applications and Future Trends in Risk Management: Real-World Applications of Risk Management in Different Industries, Emerging Trends and Technologies in Risk Management, Challenges and Opportunities in the Field, Future Directions in Risk Management Research and Practice

Textbooks:

1. "Risk Management and Financial Institutions", John C. Hull
2. "Principles of Risk Management and Insurance", George E. Rejda, Michael McNamara
3. "Risk Management: Concepts and Guidance", Carl L. Pritchard
4. "Agile Risk Management", Alan Moran
5. "Advanced Risk Analysis in Engineering Enterprise Systems", Konstantin V. Zamaraev

Reference Books:

1. "Implementing Enterprise Risk Management: Case Studies and Best Practices", John Fraser and Betty Simkins
2. "The Failure of Risk Management: Why It's Broken and How to Fix It" Douglas W. Hubbard
3. "Risk-Return Analysis: The Theory and Practice of Rational Investing (Volume One)", Harry M. Markowitz
4. "Cyber security and Cyber-Resilience: Security in the Information Age", Martin E. Hellman
5. "Financial Risk Management: A Practitioner's Guide to Managing Market and Credit Risk", Steve L. Allen



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Web Security Lab (R23MCY1255)	L	T	P	C
		0	0	3	1.5

Course Objectives:

Course Outcomes:

List of Experiments:

1. Working with Sniffers for monitoring network communication using
a)Ethereal b)Wire shark c) Snort d) tcp dump
2. Implementation and Performance evaluation of various cryptographic algorithms in C/C++/JAVA/PYTHON a)DES b)RSA.
3. Analyze the Network Traffic and port scanning using Wireshark.
4. Implement Manual SQL injection using DVWA
5. Implement Web Application Testing using DVWA.
6. Implement XSS using DVWA
7. Implement Automated SQL injection with SqlMap
8. Implement XSRF Using DVWA
9. Implement same origin policy using Pyhton/Java
10. Implement Cross-Site Scripting and Cross-Site Request Forgery using Pyhton/Java

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Constitution of India (R23MCY1257)	L	T	P	C
		2	0	0	0

Course Objectives:

- Understand the premises informing the twin themes of liberty and freedom from a civil rights perspective.
- To address the growth of Indian opinion regarding modern Indian intellectuals' constitutional role and entitlement to civil and economic rights as well as the emergence of nationhood in the early years of Indian nationalism.
- To address the role of socialism in India after the commencement of the Bolshevik Revolution in 1917 and its impact on the initial drafting of the Indian Constitution.

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

	Course Outcomes	Knowledge Level (K)#
C01	Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.	K6
C02	Discuss the intellectual origins of the framework of argument that informed the conceptualization of social reforms leading to revolution in India.	K6
C03	Discuss the circumstances surrounding the foundation of the Congress Socialist Party [CSP] under the leadership of Jawaharlal Nehru and the eventual failure of the proposal of direct elections through adult suffrage in the Indian Constitution.	K6
C04	Discuss the passage of the Hindu Code Bill of 1956.	K6
C05	Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-I: History of Making of the Indian Constitution: History, Drafting Committee, (Composition & Working)

Philosophy of the Indian Constitution- Preamble, Salient, Features

UNIT-II: Contours of Constitutional Rights & Duties: Fundamental Rights, Right to Equality, Right to Freedom, Right against Exploitation, Right to Freedom of Religion, Cultural and Educational Rights, Right to Constitutional Remedies, Directive Principles of State Policy, Fundamental Duties.

UNIT-III: Organs of Governance: Parliament, Composition, Qualifications and Disqualifications, Powers and Functions, **Executive-** President, Governor, Council of Ministers, Judiciary, Appointment and Transfer of Judges, Qualifications, Powers and Functions

UNIT-IV: Local Administration: District's Administration head: Role and Importance, Municipalities: Introduction, Mayor and role of Elected Representative CEO of Municipal Corporation, Pachayati raj: Introduction, PRI: ZilaPachayat, Elected officials and their roles, CEO ZilaPachayat: Position and role, Block level: Organizational Hierarchy (Different departments), Village level: Role of Elected and Appointed officials, Importance of grass root democracy

UNIT-V: Election Commission: Election Commission: Role and Functioning, Chief Election Commissioner and Election Commissioners, State Election Commission: Role and Functioning, Institute and Bodies for the welfare of SC/ST/OBC and women.

Text Books:

1. The Constitution of India, 1st Edition, (Bare Act), Government Publication, 1950
2. Framing of Indian Constitution, 1st Edition, Dr. S. N. Busi, Dr. B. R. Ambedkar 2015

Reference Books:

1. Indian Constitution Law, 7th Edition, M. P. Jain, Lexis Nexis, 2014

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Pedagogy Studies (R23MCY1257)	L	T	P	C
		2	0	0	0

Course Objectives:

Students will be able to:

- Review existing evidence on the review topic to inform programme design and policy making undertaken by the DfID, other agencies and researchers.
- Identify critical evidence gaps to guide the development.

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

	Course Outcomes	Knowledge Level (K)#
CO1	What pedagogical practices are being used by teachers in formal and informal classrooms in developing countries?	K1
CO2	What is the evidence on the effectiveness of these pedagogical practices, in what conditions, and with what population of learners?	K1
CO3	How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy?	K1

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction and Methodology: Aims and rationale, Policy background, Conceptual framework and terminology, Theories of learning, Curriculum, Teacher education, Conceptual framework, Research questions, Overview of methodology and Searching.

UNIT-II: Thematic overview: Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries, Curriculum, Teacher education.

UNIT-III: Evidence on the effectiveness of pedagogical practices: Methodology for the in depth stage: quality assessment of included studies, How can teacher education

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

(curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy, Theory of change, Strength and nature of the body of evidence for effective pedagogical practices, Pedagogic theory and pedagogical approaches, Teachers' attitudes and beliefs and Pedagogic strategies.

UNIT-IV: Professional development: Alignment with classroom practices and follow-up support, Peer support, Support from the head teacher and the community, Curriculum and assessment, Barriers to learning: limited resources and large class sizes

UNIT-V: Research gaps and future directions: Research design, Contexts, Pedagogy, Teacher education, Curriculum and assessment, Dissemination and research impact.

Text Books:

1. Classroom interaction in Kenyan primary schools, Ackers J, Hardman F, Compare, 31 (2): 245-261, 2001
2. Curricular reform in schools: The importance of evaluation, Agrawal M, Journal of Curriculum Studies, 36 (3): 361-379, 2004

Reference Books:

1. Teacher training in Ghana: does it count? Multi-site teacher education research project (MUSTER) country report 1, Akyeampong K, London: DFID, 2003

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Stress Management by Yoga (R23MCY1257)	L	T	P	C
		2	0	0	0

Course Objectives:

- To achieve overall health of body and mind
- To overcome stress

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

	Course Outcomes	Knowledge Level (K)#
CO1	Develop healthy mind in a healthy body thus improving social health also	K2
CO2	Improve efficiency	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT – I: Definitions of Eight parts of yoga. (Ashtanga).

UNIT – II: Yam and Niyam. Do`s and Don`ts in life.

UNIT – III: Ahinsa, satya, astheya, bramhacharya and aparigrahaShaucha, santosh, tapa, swadhyay,ishwarpranidhan.

UNIT –IV: Asan and Pranayam, Various yoga poses and their benefits for mind &body.

UNIT –V: Regularization of breathing techniques and its effects-Types of pranayam.

Text Books:

1. Yogic Asanas for Group Tarining-Part-I :Janardan Swami Yogabhyasi Mandal, Nagpur
2. Rajayoga or conquering the Internal Nature, Swami Vivekananda, Advaita Ashrama Publication Department, Kolkata

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

I Year - II Semester	Personality Development through Life Enlightenment Skills (R23MCY1257)	L	T	P	C
		2	0	0	0

Course Objectives:

- To learn to achieve the highest goal happily
- To become a person with stable mind, pleasing personality and determination
- To awaken wisdom in students

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

	Course Outcomes	Knowledge Level (K)#
CO1	Study of Shrimad-Bhagwad-Geeta will help the student in developing his personality and achieve the highest goal in life	K2
CO2	The person who has studied Geeta will lead the nation and mankind to peace and prosperity	K3
CO3	Study of Neetishatakam will help in developing versatile personality of students.	K5

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
CO1						
CO2						
CO3						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Neetisatakam-Holistic development of personality, Verses- 19,20,21,22 (wisdom), Verses- 29, 31, 32 (pride & heroism), Verses- 26,28,63,65 (virtue), Verses- 52, 53, 59 (don'ts), Verses- 71,73,75,78 (do's)

UNIT-II: Approach to day to day work and duties.
Shrimad Bhagwad Geeta: Chapter 2-Verses 41, 47, 48

UNIT-III: Chapter 3-Verses 13, 21, 27, 35, Chapter 6-Verses 5, 13, 17, 23,35,
Chapter 18- Verses 45, 46, 48



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-IV: Statements of basic knowledge.

Shrimad Bhagwad Geeta: Chapter2-Verses 56, 62, 68

Chapter 12 -Verses 13, 14, 15, 16, 17, 18

UNIT-V: Personality of Role model. Shrimad Bhagwad Geeta: Chapter2-Verses 17,
Chapter 3-Verses 36, 37, 42,

Chapter 4-Verses 18, 38, 39

Chapter18 – Verses 37, 38, 63

Text Books:

1. Srimad Bhagavad Gita, Swami Swarupananda Advaita Ashram (PublicationDepartment), Kolkata
2. Bhartrihari's Three Satakam (Niti-sringar-vairagya), P.Gopinath

Reference Books:

1. Rashtriya Sanskrit Sansthanam, New Delhi.

Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

II Year - I Semester	Cyber Security Governance (R23MCY1251)	L	T	P	C
		3	0	0	3

Course Objectives:

- Knowledge and understanding of the different theories on cyber-governance, the implications of cyberspace
- Understanding the internet for traditional notions such as sovereignty, power, war and conflict, terrorism and crime.
- Understanding the historical developments in cyber governance and how key events have led to the current state of affairs.

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

	Course Outcomes	Knowledge Level (K)#
C01	Explain the fundamental concepts and principles of the cyber Security Governance and theories of governance.	K2
C02	Demonstrate the metrics of Cyber Security Governance.	K2
C03	Explain the principal driving force for Cyber security governance is risk management, which involves mitigating risks and reducing or preventing potential impact on information resources.	K5
C04	Model the enterprise needs metric against which to judge Cyber security policy to ensure that organizational objectives are achieved.	K3
C05	Explore the Threat Intelligence Governance and Industrial Governance.	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	P01	P02	P03	P04	P05	P06
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Cyber security Governance-Principles of cyber security governance, Assessment of cyber security maturity. Theories of governance: introduction, Governance – definitions and typologies, Tools, methods and processes.



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-II: Network Device metrics-Vulnerability management, Threat management, Endpoint management, Intrusion detection and prevention (IDPS), Security incident management, Security operations centre (SOC) and related concepts.

UNIT-III: Measurement of Governance-Metrics – concepts, Application security metrics, Network security metrics, Security incident metrics, Vulnerability metrics, Service level objectives / agreement (SLO / SLA), NIST metrics.

UNIT-IV: Security analytics Governance-Basics of security analytics, Threat intelligence and governance, Data driven security governance, Impact of cognitive security on security governance.

UNIT-V: Industry Governance-Industry specific security compliance, Cyber security governance India and Other countries, NIST mandates for compliance, Security reporting basics, CISO – role and organization structure.

Text Books:

1. IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, Hayden, lance, McGraw-hill education group, 2010
2. Data-Driven Security: Analysis, 1st Edition, Visualization and Dashboards, Jacobs, Jay, and Bob Rudis, John wiley & sons, 2014

Reference Books

1. Cyber Security, Critical Infrastructure, Framework for Improving Critical Infrastructure Cyber Security, Framework, 1st Edition 2014



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

II Year - I Semester	Principles of Secure Coding (R23MCY1251)	L	T	P	C
		3	0	0	3

Course Objectives:

- Understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities.
- Knowledge of outline of the techniques for developing a secure application.
- Recognize opportunities to apply secure coding principles.

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

	Course Outcomes	Knowledge Level (K)#
C01	Outline the secure systems and various security attacks	K2
C02	Demonstrate the development of process of software leads to secure coding practices	K2
C03	Apply Secure programs and various risk in the software's	K3
C04	Classify various errors that lead to vulnerabilities	K4
C05	Design Real time software and vulnerabilities	K6

#Based on suggested Revised BTL

Mapping of course outcomes with program outcomes

	PO1	PO2	PO3	PO4	PO5	PO6
C01						
C02						
C03						
C04						
C05						

(Please fill the above with Levels of Correlation, viz., L, M, H)

UNIT-I: Introduction- Need for secure systems, Proactive security development process, Security principles to live by and threat modelling.

UNIT-II: Secure Coding in C- Character strings- String manipulation errors, String Vulnerabilities and exploits Mitigation strategies for strings, Pointers, Mitigation strategies in pointer based vulnerabilities Buffer Overflow based vulnerabilities



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

UNIT-III: Secure Coding in C++ and Java- Dynamic memory management, Common errors in dynamic memory management, Memory managers, Double –free vulnerabilities, Integer security, Mitigation strategies

UNIT-IV: Database and Web Specific Input Issues- Quoting the Input, Use of stored procedures, Building SQL statements securely, XSS related attacks and remedies

UNIT-V: Software Security Engineering- Requirements engineering for secure software: Misuse and abuse cases, SQUARE process model Software security practices and knowledge for architecture and design

Text Book:

1. Writing Secure Code, 2nd Edition, Michael Howard, David LeBlanc, Microsoft Press, 2003

Reference Books:

1. Secure Coding in C and C++, Robert C. Seacord, 2nd edition, Pearson Education, 2013
2. Software Security Engineering: A guide for Project Managers, 1st ed, Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Addison-Wesley Professional, 2008



Department of Computer Science & Engineering
University College of Engineering Kakinada (A): JNTUK Kakinada

II Year - I Semester	Security Automation (R23MCY1251)	L	T	P	C
		3	0	0	3