JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

COURSE STRUCTURE & SYLLABUS M.Tech CSE for CYBER SECURITY PROGRAMME

(Applicable for batches admitted from 2019-2020)

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

I- SEMESTER

S.No	Course Code	Courses	Category	L	T	P	C
1	MTCY1101	**Program Core-1** Principles of Cyber Security	PC	3	0	0	3
2	MTCY1102	**Program Core-2** Advanced Data Structures	PC	3	0	0	3
3	MTCY1103	**Program Elective-1** 1. Cryptanalysis 2. Cyber Crime Investigation & Digital Forensics 3. Operating System Security 4. Firewall and VPN Security	PE	3	0	0	3
4	MTCY1104	**Program Elective-2** 1. Database and Web Application Security 2. Secure Software Design and Development 3. Wireless Network Security 4. Cyberspace Operations and Design	PE	3	0	0	3
5	MTCY1105	**Research Methodology and IPR**	CC	2	0	0	2
6	MTCY1106	**Laboratory-1** Cyber Security Lab	LB	0	0	4	2
7	MTCY1107	**Laboartory-2** Advanced Data Structures Lab	LB	0	0	4	2
8	MTCY1108	**Audit Course-1***	AC	2	0	0	0
Total Credits							18

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

II- SEMESTER

S.No	Course Code	Courses	Category	L	T	P	C
1	MTCY1201	**Program Core-3** Vulnerability Assessment & Penetration Testing	PC	3	0	0	3
2	MTCY1202	**Program Core-4** Malware Analysis & Reverse Engineering	PC	3	0	0	3
3	MTCY1203	**Program Elective-3** 1. Cloud and IoT Security 2. Machine Learning 3. Data Privacy	PE	3	0	0	3
4	MTCY1204	**Program Elective-4** 1. Applied Cryptography 2. Principles of Secure Coding 3. Security Assessment and Risk Analysis	PE	3	0	0	3
5	MTCY1205	**Laboratory-3** Vulnerability Assessment & Penetration Testing Lab	LB	0	0	4	2
6	MTCY1206	**Laboartory-4** Malware Analysis & Reverse Engineering Lab	LB	0	0	4	2
7	MTCY1207	**Mini Project with Seminar**	MP	0	0	0	2
8	MTCY1208	**Audit Course-2** 1. Constitution of India 2. Pedagogy Studies 3. Stress Management by Yoga 4. Personality Development through Life Enlightenment Skills	AC	2	0	0	0
Total Credits							18

Student has to choose any one audit course listed below.

Audit Course 1 & 2:

1. English for Research Paper Writing
2. Disaster Management
3. Sanskrit for Technical Knowledge
4. Value Education
5. Constitution of India
6. Pedagogy Studies
7. Stress Management by Yoga
8. Personality Development through Life Enlightenment Skills

III-SEMESTER

S.No	Course Code	Courses	Category	L	T	P	C
1	MTCY2101	**Program Elective-5** 1. Information System Audit 2. Cyber Security Governance 3. Cyber Laws and Security Policies 4. MOOCs-1 (NPTEL/SWAYAM)-12 Week Program related to the programme which is not listed in the course structure	PE	3	0	0	3
2	MTCY2102	**Open Elective** 1. MOOCs-2 (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	MTCY2103	**Dissertation-I/Industrial Project#**	PJ	0	0	20	10
Total Credits							16

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

M. Tech. (CSE) IV SEMESTER							
S.No	Course Code	Courses	Category	L	T	P	C
1	MTCS2201	**Dissertation-II**	PJ	0	0	32	16
Total Credits							16

Open Electives offered by the Department of CSE for other Departments Students

1. Python Programming
2. Principles of Cyber Security
3. Internet of Things
4. Artificial Intelligence and Machine Learning

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

I Year - I Semester		L	T	P	C
		3	0	0	3
Principles of Cyber Security (MTCY1101)					

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

- Apply cyber security architecture principles.
- Describe risk management processes and practices.
- Appraise cyber security incidents to apply appropriate response
- Distinguish system and application security threats and vulnerabilities.
- Identify security tools and hardening techniques

UNIT–I: Introduction to Cyber security- Cyber security objectives, Cyber security roles, Differences between Information Security & Cyber security, **Cyber security Principles-** Confidentiality, integrity, &availability Authentication & non- repudiation.

UNIT–II: Information Security (IS) 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.

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

UNIT–IV: Threat Detection and Evaluation (DE): 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 Harding of operating system.

Text Books:

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

Reference Books:

1. CSX- cyber security fundamentals 2 nd edition, Published by ISACA, Cyber security, Network Security, Data Governance Security.

I Year - I Semester		L	T	P	C
		3	0	0	3
Advanced Data Structures (MTCY1102)					

Course Objective:

- The student should be able to choose appropriate data structures, understand the ADT/libraries, and use it to design algorithms for a specific problem
- Students should be able to understand the necessary mathematical abstraction to solve problems
- To familiarize students with advanced paradigms and data structure used to solve algorithmic problems
- Student should be able to come up with analysis of efficiency and proofs of correctness

Course Outcomes:

- Explain the Collision Resolution Techniques in Hashing and implement symbol table using hashing techniques
- Develop and analyze algorithms for red-black trees, B-trees and Splay trees.
- Develop algorithms for text processing applications.
- Identify suitable data structures and develop algorithms for computational geometry problems.

UNIT-I: Dictionaries-Definition, Dictionary Abstract Data Type, and Implementation of Dictionaries. Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing.

UNIT-II: Skip Lists- Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists

UNIT-III: Trees-Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees

UNIT-IV: Text Processing: Sting Operations, Brute-Force Pattern Matching, The Boyer- Moore Algorithm, The Knuth-Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries, The Huffman Coding Algorithm, The Longest Common Subsequence Problem (LCS), Applying Dynamic Programming to the LCS Problem

UNIT-V: Computational Geometry: One Dimensional Range Searching, Two Dimensional Range Searching, Constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quad-trees, k-D Trees. Recent Trends in Hashing, Trees, and various computational geometry methods for efficiently solving the new evolving problem

Text Books:

1. Data Structures: A Pseudo-code Approach, 2/e, Richard F.Gilberg, Behrouz A.Forouzon, Cengage
2. Data Structures, Algorithms and Applications in java, 2/e, Sartaj Sahni, University Press

Reference Books:

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004.
2. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley, 2002.

I Year - I Semester		L	T	P	C
		3	0	0	3
Cryptanalysis (MTCY1103)					

Course Objectives:

- To understand the importance of cryptanalysis in our increasingly computer-driven world.
- To understand the fundamentals of Cryptography
- To understand the Lattice- based cryptanalysis and elliptic curves and pairings
- To understand birthday- based algorithms for functions and attacks on stream ciphers
- To apply the techniques for secure transactions in real world applications

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

- Ability to apply cryptanalysis in system design to protect it from various attacks.
- Ability to identify and investigate vulnerabilities and security threats and the mechanisms to counter them.
- Ability to analyze security of cryptographic algorithm against brute force attacks, birthday attacks.

UNIT–I: A bird's – eye view of modern Cryptography: Preliminaries, Defining Security in Cryptography Mono-alphabetic Ciphers: Using Direct Standard Alphabets, The Caesar Cipher, Modular arithmetic, Direct Standard alphabets, Mono-alphabets based on linear transformation. Poly-alphabetic Substitution: Poly-alphabetic ciphers, Recognition of poly-alphabetic ciphers, Determination of number of alphabets, Solution of individual alphabets if standard, Poly-alphabetic ciphers with a mixed plain sequence, Matching alphabets, Reduction of a poly-alphabetic cipher to a mono-alphabetic ciphers with mixed cipher sequences.

UNIT–II: Transposition- Columnar transposition, Solution of transpositions with Completely filled rectangles, Incompletely filled rectangles, Solution of incompletely filled rectangles – Probable word method, Incompletely filled rectangles general case, Repetitions between messages; identical length messages. Sieve algorithms: Introductory example: Eratosthenes's sieve, Sieving for smooth composites

UNIT–III: Brute force Cryptanalysis- Introductory example: Dictionary attacks, Brute force and the DES Algorithm, Brute force as a security mechanism, Brute force steps in advanced cryptanalysis, Brute force and parallel computers. The birthday paradox: Sorting or not?: Introductory example: Birthday attacks on modes of operation, Analysis of birthday paradox bounds, Finding collisions, Application to discrete logarithms in generic groups.

UNIT-IV: Birthday- based algorithms for functions- Algorithmic aspects, Analysis of random functions, Number-theoretic applications, A direct cryptographic application in the context of block wise security, Collisions in hash functions. Attacks on stream ciphers: LFSR- based key stream generator, Correlation attacks, Noisy LFSR model, Algebraic attacks, Extension to some non- linear shift registers, the cube attack.

UNIT-V: Lattice- based cryptanalysis- Direct attacks using lattice reduction, Coppersmith's small roots attacks. Elliptic curves and pairings: Introduction to elliptic curves, The Weil pairing, the elliptic curve factoring method.

Text Books:

1. Elementary Cryptanalysis A Mathematical Approach by Abraham Sinkov, The mathematical Association of America (lnc).
2. Algorithmic Cryptanalysis" by Antoine joux, CRC Press'

Reference Books:

1. Algebraic Cryptanalysis, Bard Gregory, Springer, 2009
2. Cryptanalysis of Number Theoretic Ciphers, Sameul S. Wag staff, Champan & Hall/CRC.
3. Cryptanalysis: A Study of Cipher and Their Solution, Helen F. Gaines,1989

I Year - I Semester		L	T	P	C
		3	0	0	3
Cyber Crime Investigation and Digital Forensics (MTCY1103)					

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

- Acquire the definition of computer forensics fundamentals.
- Describe the types of computer forensics technology
- Analyze various computer forensics systems.
- Illustrate the methods for data recovery, evidence collection and data seizure.
- Summarize duplication and preservation of digital evidence.

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.

UNIT–III: Investigation: Introduction to Cyber Crime Investigation, Investigation Tools, e-Discovery, 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.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

Textbook:

1. Nihad A. Hassan, "Digital Forensics Basics: A Practical Guide Using Windows OS Paperback", February 26, 2019.

Reference Books:

1. Nelson Phillips and EnfingerSteuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics", Tata McGraw-Hill, New Delhi, 2006.
3. Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005

Web Reference:

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

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

I Year - I Semester		L	T	P	C
		3	0	0	3
Operating System Security (MTCY1103)					

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

- Explain the overview of operating system
- Demonstrate the Access control matrix, access control list and Lampson's access matrix
- Identify the Encryption Techniques, Authentication and Password Security issues
- Identify the Encryption Techniques and apply the real time applications
- Know the role and responsibilities of a system administrator and Create and administer user accounts on both a Linux and Windows platform

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(TB1)

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(TB2)

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(TB2)

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.(TB3)

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.(TB4)

Text Books:

1. Operating System Concepts, 9th Edition, Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Wiley Publication, 2008
2. Operating Systems: A Concept-Based Approach, 3rd Edition, Dhananjay M. Dhamdhere, McGraw-Hill, 2015
3. Windows Server 2003 Security, A Technical Reference, Roberta Bragg, Addisson-Wesley
4. Linux Administration Handbook, Second Edition, Evi Nemeth, Garth Snyder, Trent R. Hein. Prentice Hall

Reference Books:

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

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

I Year - I Semester		L	T	P	C
		3	0	0	3
Firewall and VPN Security (MTCY1103)					

Course Objectives:

- Identify and assess current and anticipated security risks and vulnerabilities
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan
- Implement/test contingency and backup plans and coordinate with stakeholders
- Monitor, report and resolve security problems

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

- To show the fundamental knowledge of Firewalls and it types
- Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization
- Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection
- Infer the design of Control Systems of SCAD, DCS, PLC's and ICS's
- Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC,DA/HAD

UNIT–I: Firewall Fundamentals: Introduction, Types of Firewalls, Ingress and Egress Filtering, Types of Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls.

UNIT–II: VPN Fundamentals: VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, Digital Certificates, VPN Authorization.

UNIT–III: Exploring the Depths of Firewalls: Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements, and Management Interfaces.

UNIT– IV: Overview of Industrial Control Systems: Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and Their Interdependencies.

UNIT– V: SCADA Protocols: Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing, Finding Vulnerabilities in HMI: software- Buffer Overflows, Shell code. Previous attacks Analysis- Stuxnet, Duqu.

Text Books:

1. Michael Stewart "Network Security, Firewalls, and VPNs" Jones & Bartlett Learning September 2010.
2. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI and SIS, Auerbach Publications, 2011.

3. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.

Reference Books:

1. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.
2. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. CRC Press, 2013.
3. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, et al. Industrial cloud-based cyber-physical systems Springer International Publishing, 2014.
4. D. Bailey, Practical SCADA for Industry. Burlington, MA: Newnes, 2003.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

I Year - I Semester		L	T	P	C
		3	0	0	3
Database and Web Application Security (MTCY1104)					

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

- Explain threats, vulnerabilities and breaches to design database
- Discuss Relational Data Model and concurrency controls and locking, SQL extensions to security
- Demonstrate the Browser security principles.
- How to provide software centric security and mobile web browser security in real time applications
- Construct the penetrating testing workflows with examples.

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

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

Reference Books:

1. Michael Gertz and SushilJajodia, "Handbook of Database Security— Applications and Trends", Springer, 2008.
2. Bhavani Thuraisingham, "Database and Applications Security", Integrating Information Security and Data Management, Auerbach Publications, 2005.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

I Year - I Semester		L	T	P	C
		3	0	0	3
Secure Software Design and Development (MTCY1104)					

Course Objectives:

- To fix software flaws and bugs in various software.
- To make students aware of various issues like weak random number generation, information leakage, poor usability, and weak or no encryption on data traffic.
- Techniques for successfully implementing and supporting network services on an enterprise scale and heterogeneous systems environment.
- Methodologies and tools to design and develop secure software containing minimum vulnerabilities and flaws.

Course Outcomes:

- Differentiate between various software vulnerabilities.
- Explain the Software process vulnerabilities for an organization.
- Demonstrate the Monitor resources consumption in software.
- Explain the Interrelate security and software development process.
- Discuss the Case study of DNS server, DHCP configuration and SQL injection attack.

UNIT-I: Secure Software Design-Identify software vulnerabilities and perform software security analysis, Master security programming practices, Master fundamental software security design concepts, Perform security testing and quality assurance.

UNIT-II: Enterprise Application Development- Describe the nature and scope of enterprise software applications, Design distributed N-tier software application, Research technologies available for the presentation, business and data tiers of an enterprise software application, Design and build a database using an enterprise database system, Develop components at the different tiers in an enterprise system, Design and develop a multi-tier solution to a problem using technologies used in enterprise system, Present software solution.

UNIT-III: Enterprise Systems Administration-Design, implement and maintain a directory-based server infrastructure in a heterogeneous systems environment, Monitor server resource utilization for system reliability and availability, Install and administer network services(DNS/DHCP/Terminal Services/Clustering/Web/Email).

UNIT-IV: Obtain the ability to manage and troubleshoot a network running multiple services, understand the requirements of an enterprise network and how to go about managing them.

UNIT-V: Handle insecure exceptions and command/SQL injection, Defend web and mobile applications against attackers, software containing minimum vulnerabilities and flaws, Case study of DNS server, DHCP configuration and SQL injection attack.

Text Books:

1. Theodor Richardson, Charles N Thies, Secure Software Design, Jones & Bartlett
2. Kenneth R. van Wyk, Mark G. Graff, Dan S. Peters, Diana L. Burley, Enterprise Software Security, Addison Wesley.

I Year - I Semester		L	T	P	C
		3	0	0	3
Wireless Network Security (MTCY1104)					

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

Course Objectives:

- To understand the concepts of network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks.
- Student should learn and Develop SSL or Firewall based solutions against security threats, employ access control techniques to the existing computer platforms such as UNIX and Windows NT.
- To learn and understand wireless technologies and apply real time applications

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

- Explain the History of wireless Technologies and Rogue Network Access Points
- Demonstrate the wireless LAN Security Protocols and SSL/TLS
- Describe the concepts of FDMA,GSM Security and Algorithm Analysis
- Explain Current and Future Technologies and Standards
- Identify the Basic specifications in Bluetooth Security.

UNIT-I: Introduction to Wireless: History of Wireless Technologies, History of Wireless Security, State of the Wireless Security Industry, **Wireless Threats:** Uncontrolled Terrain, Communications Jamming, DoS Jamming, Injections and Modifications of Data, Man-in-the-Middle (MITM) Attack, Rogue Client, Rogue Network Access Points, Attacker Equipment, Covert Wireless Channels, Roaming Issues, Cryptographic Threats

UNIT-II: Introduction to Wireless Security Protocols and Cryptography: Recovery the FUD, OSI Model, OSI Simplified, Internet Model, Wireless LAN Security Protocols, Cryptography, SSL/TLS, Secure Shell Protocols, Terminal Access and File Transfer, Port Forwarding a Word of Caution, Man-in-the-Middle of SSL/TLS and SSH, WTLS, WEP,802.1x, IP Security. **Security Considerations to Wireless Devices:** Wireless Device Security Issues, Physical Security, Information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistants (PDAS), Wireless Infrastructure

UNIT-III: Wireless Technologies and Applications: Introduction to Cellular Networks- FDMA, TDMA, CDMA, Spread Spectrum Primer, Analogy, TDMA Vs CDMA, PDC, Security Threats, GSM Security, GSM Algorithm Analysis. **Introduction to Wireless Data Networks:** Cellular Digital Packet Data (CDPD), CDPD Architecture, CDPD Security, Mobitex- Mobitex Architecture, Mobitex Security Architecture, General Packet Radio Service (GPRS)- GPRS Architecture, Security Issues, Introduction to the Wireless Application Protocol (WAP)- WAP Device, Gateway, Security Model

UNIT-IV: Wireless Standards and Technologies: Current and Future Technologies- Infrared, Radio, Spread Spectrum, OFDM, Current and Future Standards- IEEE 802, 802.11, The ABC's of 802.11, 802.11b, 802.11a, 802.11g, 802.11j, 802.11h and 5GPP, 802.11e, 802.11i, 802.11f, IEEE 802.15, IEEE 802.16, IEEE 802.1x, ETSI, Home RF, Ultra wideband Radio (UWB). **Wireless**

Deployment Strategies: Implementing Wireless LAN's- Security Considerations Common Wireless Network Applications, Enterprise Campus Designs, Wireless IST Design, Retail and Manufacturing Design, Small Office/Home Office Design (SOHO)

UNIT–V: Bluetooth Security: Basic specifications, Pico-nets, Bluetooth security architecture, Scatter-nets, Security at the baseband layer and link layer, Frequency hopping, Security manager, Authentication, Encryption, And Threats to Bluetooth security

Text Books:

1. Merritt Maxim and David Pollino, "Wireless Security", Osborne/McGraw Hill, New Delhi, 2005
2. Nichols and Lekka, "Wireless Security-Models, Threats and Solutions", Tata McGraw – Hill, New Delhi, 2006.
3. Charles P. Fleeger, "Security in Computing", Prentice Hall, New Delhi, 2009

Reference Books:

1. Behrouz A.Forouzan, —Cryptography & Network Security, Tata McGraw Hill, India, New Delhi, 2009.
2. William Stallings, —Cryptography and Network Security, Prentice Hall, New Delhi, 2006.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

I Year - I Semester		L	T	P	C
		3	0	0	3
Cyberspace Operations and Design (MTCY1104)					

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

- Explain the Concept of Cyberspace Environment and Design.
- List all the Cyberspace Operational Approaches.
- Outline the cyberspace operation and integrate it with a Joint Operations plan.
- Build Cyber Warriors and Warrior Corps
- Designing Cyber Related Commands and Organizational structures.

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 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 exercise.

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

Reference Books:

1. Paulo Shakarian et al. "Introduction of Cyber Warfare: A Multidisciplinary Approach," syngress, Elsevier 2013.
2. Jason Andress et al. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" Syngress, Elsevier 2013.

I Year - I Semester		L	T	P	C
		2	0	0	2

RESEARCH METHODOLOGY AND IPR (MTCY1105)

UNIT 1:

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

UNIT 2:

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 3:

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 4:

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

UNIT 5:

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.

REFERENCES:

(1) Stuart Melville and Wayne Goddard, "Research methodology: an introduction for science & engineering students'"
(2) Wayne Goddard and Stuart Melville, "Research Methodology: An Introduction"
(3) Ranjit Kumar, 2nd Edition, "Research Methodology: A Step by Step Guide for beginners"
(4) Halbert, "Resisting Intellectual Property", Taylor & Francis Ltd ,2007.
(5) Mayall, "Industrial Design", McGraw Hill, 1992.
(6) Niebel, "Product Design", McGraw Hill, 1974.
(7) Asimov, "Introduction to Design", Prentice Hall, 1962.
(8) (8) Robert P. Merges, Peter S. Menell, Mark A. Lemley, " Intellectual Property in New Technological Age", 2016.
(9) T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008

I Year - I Semester		L	T	P	C
		0	0	4	2
Cyber Security Lab (MTCY1106)					

Course Objectives:

- Student to get the knowledge about audit and information security management, which makes the student to get the real world experience.
- To learn and implement Data leakage in a website database

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

- Analyze and implement Audit security policy in windows environment, create a Demilitarized zone creation in Network environment
- Illustrate the Resource harvesting attack and mitigation, Window Patch management policy, Trojans and mitigation strategies
- Apply the knowledge of metasploit, Access control list creation and content filtering limiting the traffic
- Explain the Data leakage in a website database, Password policy and verification, Patch management using MBSA tool on windows machine
- Build an Audit Policy management, Media handling policy and event log analysis and Installation of Trojan, Network DOS attack and proof of bandwidth utilization

Exercise – 1:
Audit security policy implementation in windows environment.
Exercise – 2:
Create a Demilitarized zone creation in Network environment for information security.
Exercise – 3:
Implement Resource harvesting attack and mitigation.
Exercise – 4:
Implement Window Patch management policy.
Exercise – 5:
Knowing the Behaviour of Trojans and mitigation strategies.
Exercise- 6
Create a metasploit and make it to implement.
Exercise-7
Access control list creation and content filtering limiting the traffic.
Exercise-8
Data leakage in a website database and preventive measures.
Exercise-9
Password policy implementations and verification.
Exercise-10
Patch management implementation using MBSA tool on windows machine
Exercise-11
Audit Policy management for users and computers log analysis.
Exercise-12
Media handling policy implementation and event log analysis.
Exercise-13
Installation of Trojan and study of different options.
Exercise-14
Network DOS attack and proof of bandwidth utilization and preventive steps.

I Year - I Semester		L	T	P	C
		0	0	4	2
Advanced Data Structures Lab (MTCY1107)					

Course Objectives:

From the course the student will learn

- Knowing about oops concepts for a specific problem.
- Various advanced data structures concepts like arrays, stacks, queues, linked lists, graphs and trees.

Course Outcomes:

- Identify classes, objects, members of a class and relationships among them needed for a specific problem.
- Examine algorithms performance using Prior analysis and asymptotic notations.
- Organize and apply to solve the complex problems using advanced data structures (like arrays, stacks, queues, linked lists, graphs and trees.)
- Apply and analyze functions of Dictionary

Experiment 1:
Implement Multi stacks.

Experiment 2:
Implement Double Ended Queue (Dequeues) & Circular Queues.

Experiment 3:
Implement various Recursive operations on Binary Search Tree.

Experiment 4:
Implement various Non-Recursive operations on Binary Search Tree.

Experiment 5:
Implement BFS for a Graph

Experiment 6:
Implement DFS for a Graph.

Experiment 7:
Implement Merge & Heap Sort of given elements.

Experiment 8:
Implement Quick Sort of given elements.

Experiment 9:
Implement various operations on AVL trees.

Experiment 10:
Implement B: Tree operations.

Experiment 11:
Implementation of Binary trees and Traversals (DFT, BFT)

Experiment 12:
Implement Krushkal's algorithm to generate a min-cost spanning tree.

Experiment 13:
Implement Prim's algorithm to generate a min-cost spanning tree.

Experiment 14:
Implement functions of Dictionary using Hashing.

I Year - II Semester		L	T	P	C
		3	0	0	3

Vulnerability Assessment & Penetration Testing

Course Objectives:

- To identify security vulnerabilities and weaknesses in the target applications.
- To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- To test and exploit systems using various tools.
- To understand the impact of hacking in real time machines.

Course Outcomes:

- Explain Penetration testing phases
- Illustrate information gathering methodologies
- Apply System Hacking Techniques in real time applications
- Describe Bypassing WLAN Authentication

UNIT-I: Introduction-Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non Disclosure Agreement Checklist, Phases of hacking, Open-source/proprietary Pentest Methodologies

UNIT -II - Information Gathering and Scanning-
Information gathering methodologies- Foot printing, Competitive Intelligence- DNS Enumerations- Social Engineering attacks, Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration.

UNIT III - 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 IV - Advanced System Hacking:
Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Code, XSS - Stored, Reflected, DOM Based

UNIT V - Wireless Pentest:
Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Misassociation, Wireless Hacking Methodology, Wireless Traffic Analysis

Text Books:

1. Kali Linux 2: Windows Penetration Testing, 1st Edition, By Wolf Halton, Bo Weaver , June 2016 ,Packt Publishing

Reference Books:

1. Mastering Modern Web Penetration Testing By Prakhar Prasad,October 2016 Packt Publishing.
2. SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, Syngress Publication

I Year - II Semester		L	T	P	C
		3	0	0	3

Malware Analysis & Reverse Engineering

Course Objectives:

- To understand the purpose of computer intrusion programs

- 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

- Explain the characteristics of Malware and its effects on Computing systems.
- Predict the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.
- Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.
- Demonstrate the Malware functionalities.
- How to apply anti-reverse engineering in different Applications

UNIT–I: Malware Basics- General Aspect of Computer infection program, Non Self Reproducing Malware, How does Virus Operate, Virus Nomenclature, Worm Nomenclature, 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 Clam AV-Signatures.

Text books:

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

Reference Books:

1. ErciFiliol, "Computer Viruses: from theory to applications", Springer, 1st edition, 2005.

I Year - II Semester		L	T	P	C
		3	0	0	3
Cloud and IOT Security					

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

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

- Define Cloud Computing and memorize the different Cloud services and deployment models
- Assessing the financial, technological, and organizational capacity of employer's for actively initiating and installing cloud-based applications.
- Explain how IOT can be used in different Industries.
- Discuss how companies can plan for the future of technologies.
- How to apply smart applications in real world.

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 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, Raj kamal, McGraw Hill Higher Education
2. Internet of Things, A. Bahgya and V. Madisetti, Univesity Press, 2015

Reference Books:

1. Gautam Shroff, Enterprise Cloud Computing Technology Architecture Applications
2. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach
3. IOT Security Issues by Alasdair Gilchrist, O'Reilly Publishers, 2017.
4. Tim Mather, Subra Kumara swamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

I Year - II Semester		L	T	P	C
		3	0	0	3

Machine Learning

Course Objectives:

- To introduce students to the basic concepts and techniques of Machine Learning.
- To become familiar with regression methods, classification methods, clustering methods.
- To become familiar with the concepts of artificial neural networks.

Course Outcomes:

- Recognize the characteristics of machine learning algorithms and their applications to real world problems
- Able to write and evaluate hypothesis
- Apply kernel methods to solve real world problems.

Unit-I: Introduction-Towards Intelligent Machines, Well posed Problems, Example of Applications in diverse fields, Data Representation, Domain Knowledge for Productive use of Machine Learning, Diversity of Data: Structured / Unstructured, Forms of Learning, Machine Learning and Data Mining, Basic Linear Algebra in Machine Learning Techniques.

Unit-II: Supervised Learning- Rationale and Basics: Learning from Observations, Bias and Why Learning Works: Computational Learning Theory, Occam's Razor Principle and Over-fitting Avoidance Heuristic Search in inductive Learning, Estimating Generalization Errors, Metrics for assessing regression, Metris for assessing classification.

Unit-III: Statistical Learning- Machine Learning and Inferential Statistical Analysis, Descriptive Statistics in learning techniques, Bayesian Reasoning: A probabilistic approach to inference, K-Nearest Neighbor Classifier. Discriminate functions and regression functions, Linear Regression with Least Square Error Criterion, Logistic Regression for Classification Tasks, Fisher's Linear Discriminate and Thresholding for Classification, Minimum Description Length Principle.

Unit-IV: Support Vector Machines (SVM)- Introduction, Linear Discriminate Functions for Binary Classification, Perceptron Algorithm, Large Margin Classifier for linearly separable data, Linear Soft Margin Classifier for Overlapping Classes, Kernel Induced Feature Spaces, Nonlinear Classifier, Regression by Support vector Machines.

Learning with Neural Networks: Towards Cognitive Machine, Neuron Models, Network Architectures, Perceptron, Linear neuron and the Widrow-Hoff Learning Rule, The error correction delta rule.

Unit -V: Multilayer Perceptron Networks and error back propagation algorithm, Radial Basis Functions Networks. **Decision Tree Learning**: Introduction, Example of classification decision tree, measures of impurity for evaluating splits in decision trees, ID3, C4.5, and CART decision trees, pruning the tree, strengths and weakness of decision tree approach.

Textbooks:

1. Applied Machine Learning, M. Gopal, McGraw Hill Education
2. Machine Learning: A Probabilistic Perspective, Kevin Murphy, MIT Press,2012

Reference Books:

1. Pattern Recognition and Machine Learning, Christopher Bishop, Springer,2007
2. Programming Collective Intelligence: Building Smart Web 2.0 Applications - Toby Segaran
3. Building Machine Learning Systems with Python - WilliRichert, Luis Pedro Coelho
4. The Elements of Statistical Learning, Trevor Hastie, Robert Tibshirani, Jerome Friedman, Springer 2009 (freely available online)

I Year - II Semester		L	T	P	C
		3	0	0	3

Data Privacy

Course Objectives:

- The objective of this course is to create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals
- Student able to learn the concepts of confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

Course Outcomes:

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

- Discuss the concepts of privacy in today's environment.
- How automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
- Explain the knowledge of the role of private regulatory and self-help efforts.
- How emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.

UNIT-I: Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains-medical, financial, etc.

UNIT-II: Data explosion- Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness, **Protection Models**- Null-map, k-map, Wrong map

UNIT-III: Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.

UNIT-IV: Computation systems for protecting delimited data- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.

UNIT-V: Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.

Text books and References:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation,1st Edition, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

I Year - II Semester		L	T	P	C
		3	0	0	3

Applied Cryptography

Course Objectives:

- Student learns the basic concepts of symmetric cryptography and simple encryption methods.
- An understanding of the RSA cryptosystem, the mathematics used in the system, and the ability to encrypt and decrypt clear text using the system.
- To learn the properties of message authentication codes and the ability to use hash functions to build a message authentication code.

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

- Demonstrate the basics of Cryptographic protocols
- Explain the concepts of Stream Ciphers and Public Key Encryption
- Demonstrate Number Theory for Symmetric and Asymmetric Ciphers and discuss various Ciphers
- Discuss Hashing Algorithms and Message Authentication Codes
- Discuss Key-Exchange algorithms and Real world Implementations

UNIT– I: Foundations: Protocol Building Blocks, Basic Protocols, Advanced Protocols - Zero-Knowledge Proofs, Zero-Knowledge Proofs of Identity, Blind Signatures, Identity-Based Public-Key Cryptography, Key Length, Key Management, Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Ciphers, Self-Synchronizing Stream Ciphers, Cipher- Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mode, Counter Mode, Other Block-Cipher Modes, Choosing a Cipher Mode.

UNIT – II: Information Theory, Complexity Theory, Number Theory, Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field, Data Encryption Standard (DES), IDEA, CAST, Blowfish, RC5, Double Encryption, Triple Encryption.

UNIT–III: Pseudo-Random-Sequence Generators and Stream Ciphers- Linear Congruential Generators, Linear Feedback Shift Registers, Stream Ciphers using LFSRs, RC4, Feedback with Carry Shift Registers, Stream Ciphers Using FCSRs, Nonlinear-Feedback Shift Registers, Other Stream Ciphers, One-Way Hash Functions- MD5, Secure Hash Algorithm (SHA), One Way Hash Functions Using Symmetric Block, Using Public Key Algorithms, Message Authentication Codes.

UNIT– IV: Public-Key Algorithms, Knapsack Algorithms, RSA, Rabinm ElGamal, Elliptic Curve Cryptosystems, Digital Signature Algorithm (DSA), DSA Variants, Gost Digital Signature Algorithm, Discrete Logarithm Signature Schemes, Ong-Schnorr-Shamir, Schnorr, Converting Identification Schemes to Signature Schemes.

UNIT– V: Diffie- Hellman, Station-to-Station Protocol, Multiple-Key Public-Key Cryptography, Subliminal Channel, Undeniable Digital Signatures, Designated Confirmer Signatures, Kerberos, Privacy-Enhanced Mail (PEM), Message Security Protocol (MSP), Pretty Good Privacy (PGP), Smart Cards, Public-Key Cryptography Standards (PKCS).

Text Books:

1. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Bruce Schneier, John Wiley & Sons Inc, 1996
2. Cryptography and Network Security, 6th Edition, William Stallings, Pearson Education, March 2013

Reference Books:

1. Modern Cryptography Theory and Practicel, Wenbo Mao, Pearson Education, 2004
2. Cryptography and network security, Behrouz A. Forouzan, McGraw-Hill, Inc., 2008

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

I Year - II Semester		L	T	P	C
		3	0	0	3

Principles of Secure Coding

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

- List of secure systems and various security attacks
- Demonstrate the development of process of software leads to secure coding practices
- Apply Secure programs and various risk in the software's
- Classify various errors that lead to vulnerabilities
- Design Real time software and vulnerabilities

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

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

Reference Books:

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

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

I Year - II Semester		L	T	P	C
		3	0	0	3

Security Assessment and Risk Analysis

Course Objectives

- Student able to learn basic concepts of risk management
- Integrate the IRP, DRP, and BCP plans into a coherent strategy to support sustained organizational operations.
- Able understand and discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

Course Outcomes:

- Discuss the concepts of contingency strategies including data backup and recovery and alternate site selection for business resumption planning
- Describe the escalation process from incident to disaster in case of security disaster.
- Explain Designing process of a Disaster Recovery and Business Continuity Plan for sustained organizational operations.
- Discuss the concepts of cryptography encryption and cryptography key management.

UNIT-I: Security Basics-Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security counter measures education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security counter measures policy, procedures and practices, threats, vulnerabilities.

UNIT-II: Threats to and Vulnerabilities of Systems: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment

UNIT-III: Security Planning: directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for offsite processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation

UNIT-IV: Policies And Procedures: Physical Security Measures: alarms, building construction, cabling, communications centre, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms) Personnel Security Practices and Procedures: access authorization/verification (needtoknow), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing , Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs

UNIT-V: Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography encryption (e.g., point to point, network, link), cryptography key management (to include electronic key),cryptography strength (e.g., complexity, secrecy, characteristics of the key) Case study of threat and vulnerability assessment

Text Books:

1. Principles of Incident Response and Disaster Recovery, 1st Edition,Whitman & Mattord, Course Technology,2006

Web Link Reference: http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

I Year - I Semester		L	T	P	C
		0	0	4	2

Vulnerability Assessment & Penetration Testing Lab

Experiment 1:

Implement penetration testing and phases of penetration testing

Experiment 2:

Make use of different types of tools available in kali and parrot O.S

Experiment 3:

Practice different SQL injection attacks

Experiment 4:

Implement and use GHDBC and Microsoft Vulnerabilities (Common CVE)

Experiment 5:

Implement Exploit insecure file handling, upload web shells, deface using upload file mechanism

Experiment 6:

Perform XSS attacks on client side application

Experiment 7:

Implement a case on actions on-behalf users by CSRF, Test websites for Click jacking

Experiment 8:

Implement port scanning by using NMAP and other tools to find the open ports

Experiment 9:

Text for wireshark and tcp dumps to analyze various types of packets

Experiment 10:

Implement Password attacks with methods like Dictionary Files - Key-space Brute Force - Pwdump and Fgdump - Windows Credential Editor (WCE- Exercises - Password Profiling - Password Mutating

Experiment 11:

Implement metasploit frameworks

Experiment 12:

Implement Trojan horse root kits back doors

Experiment 13:

Practice ARP spoofing and buffer overflow exploitation with ETERCAP AND SHELL'S

Experiment 14:

Perform Port Redirection, SSL Encapsulation - Stunnel, HTTP CONNECT Tunneling, Proxy Tunnel, SSH Tunneling .

List of open Source software/learning Websites:

1. https://www.hackthebox.eu/
2. https://practicalpentestlabs.com/
3. https://pentesterlab.com

I Year - II Semester		L	T	P	C
		0	0	4	2

Malware Analysis & Reverse Engineering Lab

Experiment 1:
Set up a safe virtual environment to analyze malware

Experiment 2:
Quickly extract network signatures and host-based

Experiment 3:
Make Use of key analysis tools like IDA Pro, OllyDbg, and WinDbg tools analyse malware.

Experiment 4:
Choose the malware tricks to Overcome like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques

Experiment 5:
Make Use of your newfound knowledge of Windows internals for malware analysis

Experiment 6:
Interacting with malicious websites to assess the nature of their threats

Experiment 7:
Perform analysis and De-obfuscating and analysis of malwares

Experiment 8:

Implement the De-obfuscating malicious JavaScript using debuggers and interpreters

Experiment 9:
Analyzing suspicious PDF files

Experiment 10:
Examining malicious Microsoft Office documents, including files with macros

Experiment 11:
Analyzing malicious RTF document files

Experiment 12:
Install Reanimator in your Windows machine and scan the system for Malware and prepare one report for the same

Experiment 13:

Implement the Different live case studies on malware and their behaviours

Experiment 14:

Analysing different types of malwares.

List of open Source software/learning Websites:

- http://www.malware-analyzer.com
- http://resources.infosecinstitute.com/malware-analysis-basic- dynamic-techniques/#gref http:://www.remux.org

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

II Year - I Semester		L	T	P	C
		3	0	0	3

Information System Audit

Course Objectives:

- To understand the foundations of information systems auditing
- To understand the management, application control framework
- To understand about the evidence collection and evidence evaluation process

Course Outcomes:

- Explain about Foundations of information Systems Auditing and Conducting
- Evaluating the Major phases in the Systems Development Process
- Discuss the concepts of Operations management Controls Quality assurance Management Controls.
- Describe the Concurrent Auditing techniques and Audit Software
- How to Evaluate System Effectiveness

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.
The management Control Framework-I: Introduction, Evaluating the planning Function, Evaluating the Leading Function, Evaluating the 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.

Unit-II: The Management Control Framework-II: Security Management Controls, Operations management Controls Quality assurance Management Controls. **The Application Control Framework-I:** Boundary Controls, Input Controls, and Communication Controls.

Unit-III: The Application Control Framework-II: Processing Controls, Database Controls, output Controls. s

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

Unit-V: Evidence Evaluation: Evaluating Asset Safeguarding and Data Integrity, Evaluating System Effectiveness, Evaluating System Efficiency.

References Books:

1. Ron Weber, Information Systems Control and Audit, Pears
2. M. Revathy Sri ram, Systems Audit, TMH, New Delhi, 2001. Jalote: Software Project Management in Practice, Pearson Education
3. Royce : Software Project Management, Pearson Education

II Year - I Semester		L	T	P	C
		3	0	0	3

Cyber Security Governance

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

- Label the fundamental concepts and principles of the cyber Security Governance and theories of governance.
- Demonstrate the metrics of Cyber Security Governance.
- 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.
- Model the enterprise needs metric against which to judge Cyber security policy to ensure that organizational objectives are achieved.
- Explore the Threat Intelligence Governance and Industrial Governance.

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.

UNIT–II: Network Device metrics-Vulnerability management, Threat management, Endpoint management, Intrusion detection and prevention (IDPS), Security incident management, Security operations center (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. "Hayden, Lance. IT Security Metrics: A Practical Framework For Measuring Security & Protecting data. McGraw-Hill Education Group, 2010.
2. Jacobs, Jay, and Bob Rudis. Data-Driven Security: Analysis, Visualization and Dashboards. John Wiley & Sons, 2014.

Reference Books

1. Cyber Security, critical infrastructure. "Frame work for improving critical infrastructure Cyber Security." framework 1 (2014).

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

II Year - I Semester		L	T	P	C
		3	0	0	3

Cyber Laws and Security Policies

Course Objectives:

- The Objectives Of This Course Is 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

- Explain the Social And Intellectual Property Issues Emerging From 'Cyberspace.
- Explore The Legal And Policy Developments In Various Countries To Regulate Cyberspace
- Develop The Understanding Of Relationship Between Commerce And Cyberspace.
- Determine in Depth Knowledge Of Information Technology Act And Legal Frame Work Of Right To Privacy, Data Security And Data Protection.
- Apply various Case Studies on Real Time Crimes.

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.

Reference Books:

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)l, 2ndEdition, O" Reilly Media, 2006.
2. Thomas R. Peltier, Information Security policies and procedures: A Practitioner's Referencel, 2nd Edition Prentice Hall,2004.
3. Kenneth J. Knapp, Cyber Security and Global Information Assurance: Threat Analysis and Response Solutionsl, IGI Global, 2009.

Web References:

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

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: ENGLISH FOR RESEARCH PAPER WRITING

Course objectives:

Students will be able to:

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 Ensure the good quality of paper at very first-time submission

Syllabus

Units	CONTENTS	Hours
1	Planning and Preparation, Word Order, Breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness	4
2	Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticising, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts. Introduction	4
3	Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check.	4
4	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,	4
5	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	4
6	useful phrases, how to ensure paper is as good as it could possibly be the first- time submission	4

Suggested Studies:

1. Goldbort R (2006) Writing for Science, Yale University Press (available on Google Books)
2. Day R (2006) How to Write and Publish a Scientific Paper, Cambridge University Press
3. Highman N (1998), Handbook of Writing for the Mathematical Sciences, SIAM. Highman'sbook .
4. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: DISASTER MANAGEMENT

Course Objectives: -Students will be able to:

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

Syllabus		
Units	**CONTENTS**	**Hours**
1	**Introduction** Disaster: Definition, Factors And Significance; Difference Between Hazard And Disaster; Natural And Manmade Disasters: Difference, Nature, Types And Magnitude.	4
2	**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.	4
3	**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	4
4	**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.	4
5	**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.	4
6	**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.	4

Suggested Readings:

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

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: SANSKRIT FOR TECHNICAL KNOWLEDGE

Course Objectives

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

Syllabus

Unit	Content	Hours
1	Alphabets in Sanskrit, Past/Present/Future Tense, Simple Sentences	4
2	Order Introduction of roots Technical information about Sanskrit Literature	4
3	Technical concepts of Engineering-Electrical,	4
4	Technical concepts of Engineering - Mechanical.	4
5	Technical concepts of Engineering - Architecture.	4
6	Technical concepts of Engineering – Mathematics.	4

Suggested reading

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

Course Output

Students will be able to

1. Understanding basic Sanskrit language
2. Ancient Sanskrit literature about science & technology can be understood
3. Being a logical language will help to develop logic in students

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: VALUE EDUCATION

Course Objectives

Students will be able to

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

Syllabus

Unit	Content	Hours
1	Values and self-development –Social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non- moral valuation. Standards and principles. Value judgements	4
2	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	4
3	Personality and Behavior Development - Soul and Scientific attitude. Positive Thinking. Integrity and discipline. Punctuality, Love and Kindness. Avoid fault Thinking.	4
4	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	4
5	Character and Competence –Holy books vs Blind faith. Self-management and Good health. Science of reincarnation. Equality, Nonviolence ,Humility, Role of Women.	4
6	All religions and same message. Mind your Mind, Self-control. Honesty, Studying effectively	4

Suggested reading

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

Course outcomes

Students will be able to 1.Knowledge of self-development

2.Learn the importance of Human values 3.Developing the overall personality

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: CONSTITUTION OF INDIA

Course Objectives:
Students will be able to:

1. Understand the premises informing the twin themes of liberty and freedom from a civil rights perspective.
2. 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.
3. 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.

Syllabus		
Units	**Content**	**Hours**
1	**History of Making of the Indian Constitution:** History Drafting Committee, (Composition & Working)	4
2	**Philosophy of the Indian Constitution:** Preamble Salient Features	4
3	**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.	4
4	**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	4

5	**Local Administration:** District's Administration head: Role and Importance, Municipalities: Introduction, Mayor and role of Elected Representative, CE 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	4
6	**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.	4

Suggested reading

1. The Constitution of India, 1950 (Bare Act), Government Publication.
2. Dr. S. N. Busi, Dr. B. R. Ambedkar framing of Indian Constitution, 1st Edition, 2015.
3. M. P. Jain, Indian Constitution Law, 7th Edn., Lexis Nexis, 2014.
4. D.D. Basu, Introduction to the Constitution of India, Lexis Nexis, 2015.

Course Outcomes:

Students will be able to:

1. Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.
2. Discuss the intellectual origins of the framework of argument that informed the conceptualization of social reforms leading to revolution in India.
3. 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.
4. Discuss the passage of the Hindu Code Bill of 1956.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: PEDAGOGY STUDIES

Course Objectives:

Students will be able to:

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

Syllabus		
Units	**Content**	**Hours**
1	**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.	4
2	Thematic overview: Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries. Curriculum, Teacher education.	4
3	Evidence on the effectiveness of pedagogical practices Methodology for the in depth stage: quality assessment of included studies. How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy?	4
4	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.	4
5	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	4
6	**Research gaps and future directions** Research design Contexts Pedagogy Teacher education Curriculum and assessment Dissemination and research impact.	4

Suggested reading

1. Ackers J, Hardman F (2001) Classroom interaction in Kenyan primary schools, Compare, 31 (2): 245-261.
2. Agrawal M (2004) Curricular reform in schools: The importance of evaluation, Journal of Curriculum Studies, 36 (3): 361-379.
3. Akyeampong K (2003) Teacher training in Ghana - does it count? Multi-site teacher education research project (MUSTER) country report 1. London: DFID.
4. Akyeampong K, Lussier K, Pryor J, Westbrook J (2013) Improving teaching and learning of basic maths and reading in Africa: Does teacher preparation count? International Journal Educational Development, 33 (3): 272–282.
5. Alexander RJ (2001) Culture and pedagogy: International comparisons in primary education. Oxford and Boston: Blackwell.
6. Chavan M (2003) Read India: A mass scale, rapid, 'learning to read' campaign.
7. www.pratham.org/images/resource%20working%20paper%202.pdf.

Course Outcomes:

Students will be able to understand:

1. What pedagogical practices are being used by teachers in formal and informal classrooms in developing countries?
2. What is the evidence on the effectiveness of these pedagogical practices, in what conditions, and with what population of learners?
3. How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy?

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA

KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: STRESS MANAGEMENT BY YOGA

Course Objectives

1. To achieve overall health of body and mind
2. To overcome stress

Syllabus

Unit	Content	Hours
1	Definitions of Eight parts of yog. (Ashtanga)	5
2	Yam and Niyam. Do`s and Don't's in life. Ahinsa, satya, astheya, bramhacharya and aparigraha	5
3	Yam and Niyam. Do`s and Don't's in life. Shaucha, santosh, tapa, swadhyay, ishwarpranidhan	5
4	Asan and Pranayam Various yog poses and their benefits for mind & body	5
5	Regularization of breathing techniques and its effects-Types of pranayam	4

Suggested reading

1. 'Yogic Asanas for Group Tarining-Part-I" : Janardan Swami YogabhyasiMandal, Nagpur
2. "Rajayoga or conquering the Internal Nature" by Swami Vivekananda, Advaita Ashrama (Publication Department), Kolkata

Course Outcomes:

Students will be able to:

1. Develop healthy mind in a healthy body thus improving social health also
2. Improve efficiency

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY: KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

AUDIT 1 and 2: PERSONALITY DEVELOPMENT THROUGH LIFE ENLIGHTENMENT SKILLS

Course Objectives

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

Syllabus

Unit	Content	Hours
1	Neetisatakam-Holistic development of personality Verses- 19,20,21,22 (wisdom) Verses- 29,31,32 (pride & heroism) Verses- 26,28,63,65 (virtue)	4
2	Neetisatakam-Holistic development of personality Verses- 52,53,59 (dont's) Verses- 71,73,75,78 (do's)	4
3	Approach to day to day work and duties. Shrimad Bhagwad Geeta : Chapter 2-Verses 41, 47,48,	4
4	Chapter 3-Verses 13, 21, 27, 35, Chapter 6-Verses 5,13,17, 23, 35, Chapter 18-Verses 45, 46, 48.	4
5	Statements of basic knowledge. Shrimad Bhagwad Geeta: Chapter2-Verses 56, 62, 68 Chapter 12 -Verses 13, 14, 15, 16,17, 18	4
6	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	4

Suggested reading

1. "Srimad Bhagavad Gita" by Swami Swarupananda Advaita Ashram (Publication Department), Kolkata
2. Bhartrihari's Three Satakam (Niti-sringar-vairagya) by P.Gopinath, Rashtriya Sanskrit Sansthanam, New Delhi.

Course Outcomes

Students will be able to

1. Study of Shrimad-Bhagwad-Geeta will help the student in developing his personality and achieve the highest goal in life
2. The person who has studied Geeta will lead the nation and mankind to peace and prosperity
3. Study of Neetishatakam will help in developing versatile personality of students