MARRI LAXMAN REDDY
INSTITUTE OF TECHNOLOGY AND MANAGEMENT
(AN AUTONOMOUS INSTITUTION)
(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad)
Accredited by NAAC with 'A' Grade & Recognized Under Section 2(f) & 12(B) of the UGC act,1956

COURSE CONTENT

CYBER SECURITY								
I Semester: MBA								
Course Code	**Category**	**Hours/Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIE**	**SEE**	**Total**
25MB006B	**CORE**	3	0	-	3	40	60	100
Contact Classes:45	**Tutorial Classes:** Nil	**Practical Classes:** Nil				**Total Classes:** 45		
Prerequisite: Basic concepts of Information Technology								

COURSE OVERVIEW:

This course is designed to help students understand the economic objectives of firms and support optimal decision-making. Managerial Economics examines both microeconomic and macroeconomic factors, including market conditions, population growth, and overall economic growth. The course covers key topics such as production management, demand and supply analysis, cost of production, market structures, pricing methods, pricing strategies, and output decisions. It also introduces the application of mathematical and statistical tools to analyze economic data and facilitate informed managerial decision-making.

COURSE OBJECTIVES:

- Understand the fundamental principles and objectives of cybersecurity in modern organizations.
- Identify and assess types of cyber threats and understand the role of cyber laws and ethics.
- Evaluate management practices, policies, and control mechanisms for cybersecurity.
- Analyze tools, technologies, and frameworks used in cybersecurity.
- Apply cybersecurity knowledge to current trends and personal practices in digital environments.

COURSE OUTCOMES: After Completion of the course, students should be able to

1. Define and explain key cybersecurity concepts, terminologies, and frameworks.
2. Identify and classify cyber threats, threat actors, and legal considerations.
3. Apply organizational security practices, controls, and incident response plans
4. Evaluate the effectiveness of cybersecurity technologies and frameworks.
5. Formulate strategies to protect data and privacy in evolving tech contexts

UNIT-I: Foundations of Cyber security: Introduction to Information Systems, Cyberspace and Cybersecurity, Cybersecurity vs. Information Security. Key Concepts of Cybersecurity: definition, meaning and scope of cybersecurity. Key objectives of cybersecurity: confidentiality, integrity &

availability (CIA triad). Essential Security and Privacy Goals. Cybersecurity Vulnerabilities and Challenges, Common Vulnerabilities and Exposures (CVE).

UNIT-II: Cyber Threats, Crimes, and Legal Frameworks: Types of Cybercrime and Threat Actors, Motives of attackers, Cyberattack Tools and Methods, Cyber Kill Chain and Response, National and International Cybersecurity Policies, Cybersecurity Laws and Ethics, Role of Law Enforcement and Cyber Forensics, Cybercrime Investigation and Evidence Handling.

UNIT-III: Cybersecurity Management and Controls: Information Security Governance and Risk Management. Cybersecurity Management Practices, Security Policies, Procedures, and Controls, Security Incident Response and Business Continuity, Data and Application Security. Overview of Technical Controls, Physical and User Access Security, Internet of Things (IoT) Security.

UNIT-IV: Cybersecurity Tools, Technologies, and Emerging Frameworks: Cybersecurity Frameworks and Industry Standards, Cyber Resilience and Human Factor, Cryptography and Digital Signatures, Identity and Access Management (IAM), Antivirus, Email Security, Role of AI, Blockchain, and Quantum Computing in Cybersecurity.

UNIT-V: Contemporary Applications and Personal Cybersecurity: Personal Cybersecurity Best Practices, Privacy and Data Protection Regulations, Cybersecurity. Emerging Technologies: Web 3.0, 5G, APTs, Secure-by-Design and Supply Chain Security, Ethical Use of Technology and Digital Trust.

TEXT BOOKS:

- Ajay Singh. Introduction to Cybersecurity: Concepts, Principles, Technologies and Practices. Universities Press (India) Pvt. Ltd. 2023.
- Jocelyn O. Padallan. Cybersecurity. Arceler Press. 2020. (e-book)
- Susan Lincke. Information Security Planning: A Practical Approach. Springer. 2024

REFERENCE BOOKS:

- Susanne Chishti and Janob Barberis, The Fintech Book, Wiley
- David L. Shrier and Alex Pentlan, Global Fintech, The MIT Press, 2022.

ELECTRONIC RESOURCES:

1. http://www.spinger.com/gp/cyber security.com
2. http://www.en.wikipedia.rg/wiki/list_of_cyber_security.html

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology

6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. PowerPoint presentation
11. Drshya Siksha Sangrah (DSS) Videos