INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CYBER SECURITY								
I Semester: MBA								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
CMBE09	**Elective**	**3**	**0**	**-**	**3**	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisite: Basic concepts of Information Technology								
SDGs Mapped: SDG 16 (Peace, Justice and Strong Institutions)								

I. COURSE OVERVIEW:
This course is to provide with a comprehensive understanding of cybersecurity principles, threats, management practices, tools, and emerging technologies. It emphasizes both the technical and managerial aspects of cybersecurity, including risk management, legal frameworks, and personal cybersecurity. Students will learn to analyze cyber threats, implement security controls, and apply cybersecurity strategies to protect organizational and personal information in an evolving digital landscape.

II. COURSES OBJECTIVES:
The students will try to learn:

I. The foundations, key concepts, and objectives of cybersecurity.
II. The various types of cyber threats, cybercrimes, and the legal and ethical frameworks governing cybersecurity.
III. The cybersecurity management practices, risk management, and security controls.
IV. The emerging tools, technologies, and frameworks that enhance cybersecurity resilience.
V. Integrate cybersecurity best practices, personal security measures, and contemporary applications to mitigate risks in organizations and personal contexts.

III. COURSE OUTCOMES:
At the end of the course students should be able to:

CO1 Familiarize with the concepts of cybersecurity, including CIA triad, security goals, vulnerabilities, and challenges.
CO2 Analyze cyber threats, types of cybercrimes, attacker motives, and legal frameworks to ensure compliance and ethical cybersecurity practices.
CO3 Develop strategies for cybersecurity governance, risk management, and implementation of security policies, procedures, and controls.
CO4 Identify and apply technical and physical security controls, IoT security measures, and incident response protocols to protect organizational information assets.
CO5 Evaluate cybersecurity tools, cryptography, IAM systems, AI, blockchain, and emerging frameworks to strengthen digital resilience.
CO6 Apply personal cybersecurity best practices, privacy regulations, and contemporary technologies (Web 3.0, 5G, APTs) to secure digital interactions and organizational systems.

IV. COURSE CONTENT:

MODULE - I: FOUNDATIONS OF CYBERSECURITY (08)
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).

MODULE - II: CYBER THREATS, CRIMES, AND LEGAL FRAMEWORKS (10)
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.

MODULE - III: CYBERSECURITY MANAGEMENT AND CONTROLS (09)
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.

MODULE - IV: CYBERSECURITY TOOLS, TECHNOLOGIES, AND EMERGING FRAMEWORKS (10)
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.

MODULE - V: CONTEMPORARY APPLICATIONS AND PERSONAL CYBERSECURITY (08)
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.

V. TEXTBOOKS:

1. Ajay Singh, “Introduction to Cybersecurity: Concepts, Principles, Technologies and Practices”, Universities Press (India) Pvt. Ltd. 2024.
2. Jocelyn O, Padallan, “Cybersecurity”, Arceler Press. 2020. (e-book), 2022.
3. Susan Lincke, “Information Security Planning: A Practical Approach”, Springer. 2022.

VI. REFERENCE BOOKS:

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

VII. Web References:

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

VIII. E-Text Books:

1. http://www.search.gmx.net/abuteconomics/saveyourtime.com
2. http://www.archive.mu.ac.in/myweb_test/pliticalscience.com