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

COURSE CONTENT

CYBER SECURITY								
VII Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACIC12	**Elective**	3	0	0	3	30	70	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes:45**		
Prerequisite: Computer Networks								

I. COURSE OVERVIEW:

Cyber Security was designed to help learners develop a deeper understanding of modern information and system protection technology and methods. The learning outcome is simple: We hope learners will develop a lifelong passion and appreciation for cyber security, which are certain will help in future endeavors. Students, developers, managers, engineers, and even private citizens will benefit from this learning experience. Special customized interviews with industry partners were included to help connect the cyber security concepts to live business experiences.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The broad set of technical, social & political aspects of computer security.
II. The key components of cyber security and the network architecture.
III. The threats and risks within context of the cyber security and also know the operational and organizational security aspects.
IV. Different types of incidents including categories, responses and timelines for response.

III. SYLLABUS:

MODULE – I: INTRODUCTION TO CYBER SECURITY (09)

Introduction, Computer Security, Threats, Harm, Vulnerabilities, Controls, Authentication, Access Control and Cryptography, Web user side , Browser attacks , Web attacks targeting users , Obtaining user or website data , Email attacks.

MODULE – II: SECURITY IN OPERATING SYSTEM AND NETWORKS (09)

Security in Operating Systems, Security in the Design of Operating Systems, Rootkit, Network security attack, Threats to Network Communications, Wireless Network, Security, Denial of Service, Distributed Denial-of-Service.

MODULE – III: DEFENCES: SECURITY COUNTER MEASURES (09)

Cryptography in Network Security, Firewalls, Intrusion Detection and Prevention Systems, Network Management.

Databases, Security Requirements of Databases, Reliability and Integrity, Database Disclosure, Data Mining and Big Data.

MODULE – IV: PRIVACY IN CYBERSPACE (09)

Privacy Concepts, Privacy principles and policies, Authentication and privacy, data mining, privacy on the web, Email security, Privacy impacts of emerging technologies where the field is headed.

MODULE – V: MANAGEMENT AND INCIDENTS (09)

Security Planning, Business Continuity Planning, Handling Incidents, Risk Analysis, Dealing with Disaster, Emerging Technologies, The Internet of Things, Economics, Electronic Voting, Cyber Warfare, Cyberspace and the Law, International Laws, Cyber-crime, Cyber Warfare and Home Land Security.

IV. TEXT BOOKS:

1. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, "Security in Computing", 5th Edition, Pearson Education, 2015.
2. MarttiLehto, PekkaNeittaanmäki, "Cyber Security: Analytics, Technology and Automation", Springer International Publishing Switzerland 2015.

V. REFERENCE BOOKS:

1. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. George K. Kostopoulous, "Cyber Space and Cyber Security", CRC Press, 2013.

VI. WEB REFERENCES:

1. https://towardsdatascience.com/tagged/cybersecurity
2. https://towardsdatascience.com/tagged/information-security
3. https://medium.com/codex/data-science-for-cyber-security-32e2f81e15d3
4. https://www.infosecinstitute.com/skills/learning-paths/cybersecurity-data-science/