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

COURSE CONTENT

PRINCIPLES OF CYBER SECURITY								
V Semester: CSE (CS)								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
ACCD06	Elective	3	0	0	3	40	60	100
Contact Classes: 48	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 48		
Prerequisites: Essentials of Cyber Security, Computer Networks								

I. COURSE OVERVIEW:
This course provides a comprehensive introduction to the principles and practices of cyber security. It covers key topics including threats, vulnerabilities, security layers, authentication, and cryptographic controls. Students will explore various cyber attacks and corresponding countermeasures, and gain foundational knowledge in digital forensics, privacy issues, and cyber laws. The course also delves into practical aspects of network and database security, incident handling, and the impact of emerging technologies such as IoT and big data. Emphasis is placed on real-world applications and developing a security-first mindset essential for protecting digital assets and infrastructures.

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

I The fundamental concepts of cyber security, including threats, vulnerabilities, controls, and cryptographic techniques to protect digital systems and user data.

II The principles of digital forensics, cyber laws, and regulatory frameworks to analyze cyber incidents and understand legal implications.

III The effective countermeasures, security planning strategies, and privacy preservation techniques to secure networks, databases, and emerging technologies such as IoT and big data.

III. COURSE OUTCOMES:
After successful completion of the course, students should be able to:

CO1 Analyze various types of cyber-attacks such as browser-based, email-based, and web user-targeted attacks.

CO2 Apply digital forensic technique es to investigate cyber incidents and recover digital evidence, following standard forensic procedures and lifecycle.

CO3 Implement security mechanisms such as cryptography, firewalls, intrusion detection/prevention systems, and secure database management.

CO4 Demonstrate awareness of privacy concerns in cyberspace, including data mining, web privacy, and the impact of emerging technologies.

CO5 Develop strategic plans for cyber security management, including incident response, business continuity, risk analysis, and understanding of cyber laws and global legal frameworks.

CO6 Analyze and evaluate various types of cyber-attacks such as browser-based, email-based, and web user-targeted attacks.

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION TO CYBER SECURITY (10)
Basic Cyber Security Concepts, layers of security, Vulnerability, 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: CYBER AND DIGITAL FORENSICS (10)
Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics.

MODULE – III: DEFENCES: SECURITY COUNTER MEASURES (10)
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 Homeland Security.

V. TEXTBOOKS:

1. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, “Security in Computing”, 5th Edition, Pearson Education, 2015.
2. B. Gupta, D.P. Agrawal, HaoxiangWang, “Computer and Cyber Security: Principle s, Algorithm, Applications and Perspectives”, CRC Press, ISBN 9780815371335, 2018.

VI. REFERENCE BOOKS:

1. Chowan-Hwa(john) Wu,J. David Irwin, “Introduction to Cyber Security”, CRC Press T&F Group Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.
2. George K. Kostopoulous, “Cyber Space and Cyber Security”, CRC Press, 2018.

VII. ELECTRONIC RESOURCES:

1. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12r1.pdf
2. https://owasp.org/
3. https://www.coursera.org/learn/cyber-security-basics

VIII. MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech-talk 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. E-Learning Readiness Videos (ELRV)