



INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

FOUNDATIONS OF CYBER SECURITY								
VI Semester: CSE (CS)								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
ACCD16	Elective	L	T	P	C	CIA	SEE	Total
		3	0	0	3	40	60	100
Contact Classes: 48	Tutorial Classes: Nil	Practical Classes: Nil			Total Classes: 48			
Prerequisites: Computer Networking and Operating Systems								

I. COURSE OVERVIEW:

This course introduces the principles of cyber security, emphasizing the importance of protecting information assets. Topics include threats, vulnerabilities, risk management, cryptographic principles, and strategies for secure computing environments. Students will gain foundational knowledge to address cyber security challenges in modern digital systems.

II. COURSE OBJECTIVES:

The students will try to learn:

- I The understanding of fundamental concepts of cyber security, including threats and vulnerabilities
- II The exploration of the role of cryptographic techniques in data protection
- III The learning of strategies for secure system design and architecture.
- IV The identification of best practices for risk management and incident response

III. COURSE OUTCOMES:

At the end of the course, students should be able to:

- CO1 **Understand** key concepts and principles of cyber security.
- CO2 **Apply** cryptographic methods to secure communication and data.
- CO3 **Analyze** threats and develop strategies to mitigate risks.
- CO4 **Design** secure systems by implementing access control mechanisms.
- CO5 **Evaluate** security incidents and formulate response plans.
- CO6 **Demonstrate** knowledge of ethical and legal aspects in cyber security.

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION TO CYBER SECURITY (09)

Cyber security Concepts, Threats, and Vulnerabilities. The CIA Triad (Confidentiality, Integrity, Availability), Security Attacks: Passive, Active, Insider, and Outsider.

MODULE – II: CRYPTOGRAPHY AND DATA SECURITY (10)

Introduction to Cryptography, Symmetric vs. Asymmetric Cryptography, Hash Functions, Digital Signatures, Public Key Infrastructure (PKI).

MODULE – III: NETWORK SECURITY AND SYSTEM DESIGN (09)

Firewalls, Intrusion Detection and Prevention Systems (IDPS), Virtual Private Networks (VPNs), Security in Operating Systems, Secure System Design Principles.

Fundamentals of System Design, Scalability and Load Distribution, Database and Storage Systems

MODULE - IV: RISK MANAGEMENT AND INCIDENT RESPONSE (10)

Risk Assessment Techniques, Security Policy Development, Incident Detection and Handling, Business Continuity Planning, Disaster Recovery Strategies

MODULE – V: ETHICS AND LEGAL IMPLICATIONS (10)

Cyber security Laws and Regulations, Ethical Hacking Principles, International Cyber security Frameworks, Privacy Concerns, Emerging Trends in Cyber security (AI, IoT, Blockchain)..

V. TEXTBOOKS:

1. William Stallings, “Network Security Essentials: Applications and Standards”, Pearson Education, 6th Edition, 2017.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger, “*Security in Computing*”, Pearson Education, 5th Edition, 2015.

VI. REFERENCE BOOKS:

1. Nina Godbole and Sunit Belapure, “Cyber Security: Understanding Cyber Crimes, Computer Forensics, and Legal Perspectives”, Wiley India, 1st Edition, 2011.
2. Thomas R. Peltier, “Information Security Risk Analysis”, CRC Press, 3rd Edition, 2012.

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)