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

COURSE CONTENT

ESSENTIALS OF CYBER SECURITY							
III Semester: CSE(CS)							
Course Code	**Category**	**Hours/Week**			**Credits**	**Maximum Marks**		
ACCD01	**Core**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	-	-	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisite: Nil								

I. COURSE OVERVIEW:

Cyber security course gives the comprehensive overview of the cybersecurity policies and concepts and learn the challenges in designing a security program. This course contains basic cyber security concepts, laws, forensic investigation challenges, cyber-crimes in wireless devices, organizational implications and cybercrime mini-cases. The security model of cyber security will help the learner to develop an appropriate planning for organizations to safe guard themselves from cyberattacks.

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

I   The awareness on cyber-attacks, cyber-crimes, and cyber security.
II   The knowledge on cyber forensics and Digital Forensics within context of the cyber security.
III   The security model and analyze them before being used in many applications.
IV   The Financial and Credit card Frauds in Cyber Domain

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

CO1   Explain the basic Cyber Security Concepts to overcome the cyber-attacks.
CO2   Identify the cyberspace and the law to offer reliable legal inclusiveness to facilitating registration of real-time records.
CO3   Identify the forensic investigation and challenges in computer forensics to gather and preserve evidence.
CO4   List out various Organizational security Policies and Measures insecurity issues of mobile computing domain
CO5   Demonstrate the cost of cybercrimes and IPR issues to detect and recover internal costs in an organization.
CO6   Extend briefly about the cybercrime mini-cases examples to know the real world case studies.

IV. COURSE CONTENT:

Module I - Introduction to Cyber Security (10)
Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

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 - Cyber Crime : **Mobile and Wireless Devices (09)**
Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices. Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops.

Module IV - Social Media Overview and Security (09)
Introduction: cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations.

Module V – Cyber Frauds and Mini-Cases (09)
Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. Mini-Cases: The Indian Case of online

V. TEXT BOOKS:

1. Nina Godbole and SunitBelpure, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley publications, 2018.
2. B.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. James Graham, Richard Howard and Ryan Otson, "Cyber Security Essentials", CRC Press.
2. Chwan-Hwa(john) Wu,J. David Irwin, "Introduction to Cyber Security", CRC Press T&F GroupGambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

VII. MATERIAL ONLINE:

1. Course template
2. Tech-talk topics
3. Assignments
4. Open end experiments
5. Definition and terminology
6. Tutorial question bank
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. Early lecture readiness videos (ELRV)
11. Power point presentations