GOKARAJU RANGARAJU INSTITUTE OF ENGINEERING AND TECHNOLOGY
CYBER SECURITY
(Professional Elective –V)

Course Code: GR20A4115 **L/T/P/C:3/0/0/3**
IV Year II Semester

Pre-requisites:
Students are expected to have knowledge in

1. Basic communication methods.
2. Knowledge about cyber crimes.
3. Security primitives.

Course Objectives:

1. Learn about cybercrimes and classifications
2. Identify cyber offences and legal perspectives.
3. Understand the cybercrimes related to mobile and wireless devices.
4. Study the tools and methods used in cybercrimes
5. Know the Security Risks and threats for Organizations.

Course Outcomes:

1. Obtain firm understanding on basic terminology and concepts of cybercrimes.
2. Analyze different types of attacks.
3. Deal with the security challenges posed by mobile devices for develop encryption algorithm.
4. Implement the tools to handle security challenges.
5. Evaluate the associated challenges and the cost of cybercrimes in Organizations.

UNIT I
Introduction to Cybercrime: Introduction, Cybercrime and Information Security, Cybercriminals, Classifications of Cybercrimes and Cybercrime: The legal Perspectives and Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes.

UNIT II
Cyber Offenses: Introduction, How Criminals plan the Attacks, Types of attackers, Cyber stalking, Cyber cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.

UNIT III
Cybercrime: Mobile and Wireless Devices: 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, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in

Mobile Computing Era, Laptops.

UNIT IV

Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horse and Backdoors, Steganography, DoS and Types of DDoS attacks, SQL Injection, Buffer Overflow.

UNIT V

Cyber Security: Organizational Implications 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.

Text Books:

1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole and Sunil Belapure, WileyINDIA.

References:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security, Chwan-Hwa (john) Wu,J.David Irwin.CRC Press T&F Group.