Department of Computer Science

Cyber Awareness (SEC)

Semester II

UNIT -1 : INTRODUCTION TO CYBER AWARENESS

- Overview of cyber awareness (Definition, Scope, Importance, Key concepts and Terminology)
- Types of Cyber Threats (Malware, Ransomware, Spyware and adware)
- Impact of Cyber Threats on Individuals (Identity theft, Financial Loss, Privacy Invasion)
- Impact of Cyber Threats on Organizations (Data Breaches, Business Disruption, Reputational Damage)
- Proactive Security Measures (Risk Assessment, Security Policies and Procedures, Incident Response Planning)

UNIT -2 : PASSWORD SECURITY AND MANAGEMENT

- Identifying the value of personal information
- Exploring risks due to compromised credentials
- Consequences of having weak passwords
- Strategies for creating strong and unique passwords
- Securely managing and storing passwords
- Practices for safeguarding personal information from outside world

UNIT -3 : INTERNET AND EMAIL SECURITY

- Good vs Bad browsing practices
- Safe browsing practices
- Common online threats to avoid
- Identifying and avoiding phishing attacks
- Strategies for securing email communications and attachments
- Introduction to secure messaging platforms for enhanced privacy

UNIT -4 : SAFE BROWSING PRACTICES

- Safe browsing habits and recognizing phishing attempts
- Importance of regular software updates and patching
- Two-factor authentication and its role in enhancing security
- Secure online shopping and financial transactions

UNIT -5 : ETHICAL ONLINE BEHAVIOR AND DIGITAL CITIZENSHIP

- Exploring the concept of digital citizenship and responsible online behavior
- Strategies for managing and maintaining a positive online reputation
- Ethical considerations when creating and sharing digital content
- Recognizing the long-term impact of online actions and fostering a culture of digital respect