**COURSE CONTENT**

**UNIT 1 – Basics of Computers (History of Computers)**

1. Brief History
2. Definition of the computer
3. Types of computers
4. Characteristics of a computer
5. Basic understanding of data processing
6. The concept of data and information
7. Methods of data processing

**UNIT 2 - Classification of Computers.**

1. Classification based on signal type
   * Digital computer
   * Analog computer
   * Hybrid computer
2. Classification by purpose

* Special purpose
* General purpose

1. Classification by capacity
   * Main frame
   * Mini computers
   * Microcomputers

**UNIT 3 - Introduction to Computer Hardware (Basic Input/Out System (BIOS))**

1. Peripheral devices
2. Input devices
3. Output devices
4. Storage devices
5. Processing devices
6. Auxiliary devices (UPS, Air conditioner, Voltage stabilizer)

**UNIT 4 – Computer Software**

1. System Software
2. Operating Software
   1. Types of Operating Systems
   2. Characteristics of Operating System
3. Application Software
4. Utility Software

**UNIT 5 – Computer Network**

1. Types of Networks
2. The Internet,
3. Www,
4. Web browsers,
5. Servers, etc

**====================================================================**

**UNIT 6- Computer Security/ Virus**

1. **Introduction to Computer Security:**

Providing an overview of what computer security encompasses, including protecting hardware, software, and data from unauthorized access, destruction, or alteration.

* 1. Cyber Threat Landscape: Exploring the current landscape of cyber threats, including malware, ransomware, phishing, and social engineering attacks.
  2. Types of Attacks: Detailing common types of cyber-attacks such as Denial of Service (DoS), Man-in-the-Middle (MitM), and SQL injection attacks, among others.
  3. Security Principles and Best Practices: Discuss fundamental security principles such as confidentiality, integrity, and availability (CIA), as well as best practices for securing systems and networks.
  4. Encryption and Cryptography: Explaining the role of encryption and cryptography in securing data and communications, including symmetric and asymmetric encryption algorithms.

1. **Computer virus**
   1. Understanding Computer Viruses: Explaining the nature of viruses, how they infect systems, and their various forms (e.g., file infectors, boot sector viruses, macro viruses).
   2. Modes of Transmission: Detailing how viruses spread, including through infected files, email attachments, removable media, and network connections.
   3. Damage and Effects: Discuss the potential damage caused by viruses, such as data loss, system corruption, and unauthorized access to sensitive information.
   4. Detection and Prevention: Exploring methods for detecting and preventing virus infections, including antivirus software, regular system updates, and user education on safe computing practices.

**UNIT 7 – Ethics in Computing**

1. Privacy and Security Issues
2. Intellectual Property
3. Social Impact of Computing
4. **Introduction to Ethics in Computing**: Providing an overview of the ethical considerations and principles relevant to the field of computing, including the impact of technology on society and individuals.
5. **Privacy and Data Protection**: Discuss the ethical implications of collecting, storing, and processing personal data, as well as the importance of privacy safeguards and data protection laws.
6. **Intellectual Property**: Addressing ethical issues related to intellectual property rights, including copyright infringement, software piracy, and the fair use of digital content.
7. **Cybersecurity Ethics**: Examining ethical considerations in cybersecurity practices, such as responsible disclosure of security vulnerabilities, ethical hacking, and the ethics of cyber warfare.