**UNIT 1 MODULE 2: TOPICS**

1. **INFORMATION TECHNOLOGY SYSTEMS:**
   1. Definition of an I.S.
   2. Types of I.S.
   3. Examples
2. **COMPONENTS OF AN INFORMATION TECHNOLOGY SYSTEM:**
   1. Hardware def.,
   2. Software def.,
   3. Network def.,
   4. People - Users def. (end-users, IT professionals)
   5. Procedures
3. **PURPOSE AND FUNCTIONS OF HARDWARE COMPONENTS:**
   1. Categories of hardware components
      1. Input devices
      2. Output devices
      3. Storage devices (primary and secondary)
      4. Processor
   2. Peripheral devices
   3. Interaction between hardware components
4. **PURPOSE AND FUNCTIONS OF SOFTWARE COMPONENTS:**
   1. Systems software
      1. Function of systems software
      2. Types of system software
         1. Operating system
         2. Software drivers
         3. System Utility software
            1. Language Translators
            2. Anti-virus
            3. Disk defragmenter
            4. Backup
            5. Error checking
            6. File compression
            7. File translation
            8. Keeping configuration files
   2. Application software ( two categories – generic or task specific)
      1. General purpose software (generic software packages)
      2. Integrated software (generic software packages)
      3. Taylor-made or custom written software (task specific)
      4. Specialized / specialist software ( task specific)
   3. Software categories:
      1. Proprietary software – this is the programs and data currently used by the business or organization
      2. Open source software –
   4. Information systems:
      1. Types of information systems:
         1. Embedded systems (intelligent appliances)
         2. Monitoring and control systems
         3. Data processing systems
         4. Management information systems
         5. Decision support systems
         6. Executive information systems
         7. Expert systems
      2. Data warehouses
      3. Definitions
      4. Examples
      5. Major input and output from each type of information system such as:
         1. Data
         2. Information
         3. Processed transactions
         4. Reports (detailed, summarized, exception, ad hoc)
5. **THE VARIOUS STAGES OF THE SDLC AND SOFTWARE ENGINEERING:**
   1. SDLC Stages:
      1. Preliminary survey
      2. Feasibility study
      3. Detailed analysis and fact finding
      4. System Design and Development
      5. Implementation
      6. Maintenance and review
   2. Deliverables / output of each stage
      1. System proposal
      2. Project plan
      3. Various diagrams and charts
      4. Information system (software) test plans
      5. Conversion plans
      6. Documentation
         1. User manual
         2. Technical manual
6. **TOOLS USED IN THE DIFFERENT STAGES OF THE SDLC:**
   1. Questionnaires
   2. Interviews
   3. Observations
   4. Review/ investigation of printed material
   5. Research
   6. ER diagrams
   7. Data flow diagrams
   8. Process models
   9. Object models
   10. Decision tables and trees
   11. Computer-aided software engineering (CASE) tools
   12. Gantt charts
   13. Prototypes
   14. Flowcharts
   15. Pseudo code
   16. Programming languages
7. **PURPOSE AND FUNCTIONS OF NETWORK COMPONENTS:**
   1. Types of networks
      1. LAN
      2. WAN
      3. MAN
      4. VPN
      5. Intranet
      6. Extranet
   2. Configuration
   3. Topologies
   4. Transmission media (wired vs. wireless)
      1. Wired
         1. Fibre-optic
         2. Unshielded twisted pair (UTP)
      2. Wireless
         1. Wi-Fi
   5. Hotspots
   6. Protocols
   7. Network security
      1. Firewalls
8. **EXPLAIN THE ROLES OF USERS:**
   1. IT professionals
   2. End users
   3. Expert users
   4. Novice users
9. **THE VARIOUS FEATURES ASSOCIATED WITH THE COMPONENTS OF AN INFORMATION TECHNOLOGY SYSTEM:**
   1. Speed
   2. Efficiency
   3. Portability
   4. Maintainability
   5. Storage
   6. Transmission
10. **INTERRELATIONSHIP BETWEEN THE COMPONENTS IN AN INFORMATION TECHNOLOGY SYSTEM:**
    1. Hardware
    2. Software
    3. Network
    4. Users
11. **DESCRIBE THE DIFFERENT TYPES OF HCI:**
    1. Forms
    2. Menu
    3. Command line
    4. Natural language
    5. Graphical user interface
    6. Speech and direct manipulation
12. **DISTINGUISH BETWEEN DIFFERENT TYPES OF HCI:**
    1. Forms
    2. Menu
    3. Command line
    4. Natural language
    5. Graphical user interface
    6. Speech and direct manipulation
13. **DESCRIBE WAYS IN WHICH A USER’S CHARACTERISTICS REQUIRE ADAPTATION OF A USER INTERFACE TO INCREASE EFFECTIVENESS:**
    1. User characteristics:
       1. Age
       2. Education
       3. Differently abled
       4. Cultural differences
       5. Non-visual interfaces
       6. Sensors
    2. Differences in accessibility features
14. **COMPARE VARIOUS SECURITY MECHANISMS:**
    1. Physical access control vs. Logical access control measures and procedures
       * 1. Logical access control measures
            1. User ID and password
            2. Encryption
            3. Antivirus software
            4. Firewall software etc.
         2. Physical access control measures
            1. Lock
            2. Swipe card
            3. Firewall hardware
            4. Biometric device etc.
15. Passwords ( characteristics of an effective password – not obvious, length, mixed case, alphanumeric)
16. Authentication
17. Encryption (encoder, decoder)
18. Swipe or key cards
19. Biometric
20. Data integrity
21. Backing up – media, how often, test backup to see if it works.
22. **EXPLAIN THE MEANING OF TERMS RELATED TO THE SECURITY OF INFORMATION TECHNOLOGY SYSTEMS:**
    1. Data security
    2. Passwords
    3. Authentication
    4. Encryption
    5. Data corruption
    6. Data integrity
    7. IT security policy (procedures)
       1. **Keep user ID and password safe**: this should be given only to persons who are granted access to the computer system. Kept safe by user – not disclosing this to others, inadvertently or otherwise so that unauthorized persons cannot go on to the systems to cause harm.
       2. **Logging off computers when not in use:** unauthorized persons cannot gain access to the computer still when the authorized user is away from their workstation.
       3. **Having antivirus software that runs automatically:** so that it is not up to the user to remember to run the antivirus software so that any viruses will be discovered once the antivirus database has been updated.
       4. **Encrypting data or email being sent over a communications line:** so that if the data/ information is intercepted by a hacker, they must know the encryption method used and have the decoder in order to be able to interpret the data/information
       5. **Physical security (swipe cards, door locks):** give only to authorized persons and ensure that it is kept safe so that unauthorized persons cannot gain access to the computer area. After passing through the doors it should be locked so that unauthorized persons cannot slip in the door.
23. **DESCRIBE THE STRUCTURE OF THE WORLD WIDE WEB (WWW) AS INTERCONNECTED HYPERTEXT DOCUMENTS:**
    1. Hyperlinks
    2. Homepage
    3. Web page vs. website
    4. Hypertext transfer protocol (HTTP)
    5. Universal resource locator (URL)
    6. Hypertext markup language (HTML)
    7. Extensible markup language (XML)
    8. IP addressing vs. domain name
24. **DISCUSS INTERNET STANDARDS:**
    1. Internet standards:
       1. Hypertext transfer protocol (HTTP)
       2. Transfer control protocol/ internet protocol (TCP/IP)
    2. Specifications
    3. Guidelines
    4. Software and tools