CTI 120: NETWORK & SECURITY FOUNDATION

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course introduces students to the Network concepts, including networking terminology and protocols, local and wide area networks, and network standards. Emphasis is placed on securing information systems and the various implementation policies. Upon completion, students should be able to perform basic tasks related to networking mathematics, terminology, media and protocols.
Course Hours per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completing requirements for this course, the student will be able to:

A. Perform basic calculations necessary for network operations.
    1. Identify network components and topologies
    2. Identify address and naming systems
    3. Configure computers for network access
B. Identify the components of local and wide area networks.
    1. Identify network requirements
    2. Verify device configurations
    3. Verify security and connectivity requirements
C. Identify security risks to a networked information system.
    1. Explain core security concepts
    2. Identify security terminology and models
    3. Identify information and network security components
    4. Identify elements of cryptography
    5. Describe access control and authentication components
    6. Identify attacks against software and service

OUTLINE OF INSTRUCTION:

I. Network Infrastructures
    A. Internet, intranet and extranet
    B. Local area networks (LANs)
    C. Wide area networks (WANs)
    D. Wireless networks (WLANs)
    E. Network topologies and access methods

II. Network Hardware
    A. Switches

B. Routers
C. Media

III. Protocols and Services
A. OSI model
B. IPv4 and IPv6
C. Name resolutions
D. Networking services
E. TCP/IP

IV. Security Layers
A. Core security principles
B. Physical security
C. Internet security
D. Wireless security

V. Operating System Security
A. User Authentication
B. User Access Control (UAC)
C. Password policies
D. Encryption
E. Malware

VI. Network Security
A. Firewalls
B. Network isolation
C. Protocol security

VII. Software Security
a. Client protection
b. E-mail protection
c. Server protection