UNIVERSITY OF DELTA, AGBOR, NIGERIA
COMPUTING
COMPUTER SCIENCE
B.Sc. Information and Communication Technology

UNIDEL-ICT 206: Information & Network Security (3 Units; Compulsory; LH 45)

Senate-approved Relevance
The training of high-skilled graduates who are capable to apply key security issues and procedures in handling computer and mobile communication networks. This is in tandem with the mission and vision of UNIDEL of producing students with demonstrable potentials and skills in the area of Risk Assessment and Security Policies; and security in Mobile Communication Networks which will benefit the immediate community of Delta state and Nigeria in general.

Overview
Network has advanced and has grown into a global phenomenon to become an integral part of our daily lives. The internet connects the world on a social, business, and government level. So much information is stored and transferred online that the internet has become a target for criminals. Any devices connected to the internet must be protected from authorized disclosure using tools prescribed by the discipline of information security. Network and information security gives you the knowledge and skills needed to equip you with technical knowledge of current and emerging technologies. It encompasses all the steps taken to protect the integrity of a computer network and data or information within it. Network security is important because it keeps sensitive data safe from cyberattacks and ensures the network is usable and trustworthy.

A study of key security issues and procedures in computer and mobile communication network. The study covers the different types of network. Threats to computer networks through exploitation of network infrastructure design weaknesses. Security flaws in the network infrastructure protocols. Security of content in computer network services. Risk assessment and security policies; and security in mobile communication networks. Procedures will include: network intrusion detection and forensics technologies. Cryptographic and authentication systems, capability and access control mechanisms, and new developments in Internet routing and transport protocols. Secure mail, directory, and multimedia multicast services. Current trends and research in security policies and technologies will also be discussed.

Objectives
The objectives of this course are to:(i) Explain how information security is carried out in an organization (ii) Determine external and internal threats to an organization. (iii) Identify different threats to an organization (iv) Analyze the different threats discovered in an organization. (v) Identify fundamentals of secret and public cryptography. (vi) Construct protocols for security services, (vii) Acquire network security threats and countermeasures techniques (viii) Identify network security designs using available secure solutions (such as PGP, SSL, IPSec, etc)

Learning Outcomes

Upon completion of the course, the students will be able to: (i) Identify different forms of information passage (ii) List various types security threats (iii) Identify different types of data breaches (iv) Identify data privacy (v) Evaluate different types of cryptography solutions (vi) Demonstrate the use of cryptographic algorithms (vii) Construct cryptographic techniques to solve e-security threats.

Course Content

Key security issues and procedures in computer and mobile communication network. Threats to computer networks. Security flaws. Defensive programming. Infrastructure protocols. Risk Assessment and Security policies. Cryptography. Public-key infrastructure. Secure Signature. Certification. SSL. HTTPS. File encryption. Hash-based message. Authentication code Session IDs. Hashing. Multi-Factor Authentication. Network security. VPNs. IPSEC. Wireless security. Blockchain. Biometrics. Quantum cryptography.

Minimum Academic Standard

NUC minimum academic standard requirements for facilities.