UNIDEL-ICT 404: Systems Security (3 Units; **Compulsory**; LH=30; PH=45)

Senate-approved Relevance
The training of high-skilled graduates who are knowledgeable system security and will have the ability to analyze, develop the integration, testing, operation, and maintenance of systems security in Nigeria is in tandem with the vision and mission of University of Delta, Agbor of producing well motivated, skilfull graduates that are capable of exhibiting expertise in proffering solutions for the workplace of tomorrow. This entails producing computing graduates with demonstrable potentials and skills to analyze and report organizational security posture trends, analyse and report system security posture trends, apply security policies to meet security objectives of the system, assess adequate access controls based on principles of least privileges in Delta State, Nigeria, and the world at large. The relevance of this is seeing in computing graduates of the University of Delta, Agbor being able to develop and strategically ensure system security for any organization of interest in Delta, Nigeria and the world in general.

Overview
The objective of system security is the protection of information and property from theft, corruption, and other types of damage while allowing the information and property to remain accessible and productive. System security includes the development and implementation of security countermeasures. There are a number of different approaches to computer system security, including the use of a firewall, data encryption, passwords, and biometrics.
The objectives of the course, learning outcomes, and course synopsis are provided to address this need.

Objectives
The objectives of this course are to: (i) describe the various types of malicious code, such as viruses, worms, and trapdoors (ii) identify programming techniques for enhanced security; (iii) explain the various controls available for protection against internet attacks; (iv) describe the different ways of providing authentication of a user or program; (v) describe the mechanisms used to provide security in programs, operating systems, databases, and networks; (vi) describe the background, history, and properties of widely-used encryption algorithms; (vii) describe legal, privacy, and ethical issues in computer security; (viii) explain the typical set of tasks required of an information security professional; and (ix) describe the principles of steganography and watermarking

Learning outcomes
Upon completion of this course, students should be able to: (i) describe four types of malicious code; (ii) describe two programming techniques for enhanced security; (iii) explain four controls for protection against internet attacks; (iv) describe four different ways of providing authentication of a user or program; (v) describe two mechanisms each to provide security in programs, operating systems, databases and networks; (vi) describe the background, history and properties of widely-

used encryption algorithms; (vii) describe legal, privacy and ethical issues in computer security; (viii) explain two set of tasks required of an information security professional; and (ix) describe the principles of steganography and watermarking

Course Contents
System vulnerabilities. Applied cryptography. Host-based and network-based security. Privacy. Anonymity. Usability. Security economics. Risks and vulnerabilities. Policy formation. Controls and protection methods. Law and privacy issues. Threat models and attacks. Techniques for achieving security. Operating systems security. Capabilities. Information flow control. Language security. Network protocols. Hardware security. Security in web applications.
Lab Work: Students will design, implement and compromise a secure web server and web application in a group project. Hands-on experiences on some basic attacks using isolated VMs and simulated hardware.

Minimum Academic Standards

NUC minimum academic standard requirements for facilities.