## COURSE STRUCTURE

**Name of Course:** CYBERSECURITY FUNDAMENTALS

**Course Code:** DCS2110

**Credit Hours:** 4

**Prerequisite/co-requisite:** ICT1105 Fundamentals of Networking

**Summary:**

The unit provides an introduction to cyber security, focusing on the threats and vulnerabilities towards computer systems, networks and information assets. The threats and vulnerabilities are complemented through the examination of countermeasures that can be used to minimize the associated security issues. The unit covers a wide range of topics including; malicious software, authentication and access control, encryption, operating system security, information classification, privacy, and internet-centric concepts.

**Course Learning Outcomes:**

Upon completing this course, the students will be able to:
CLO1: Describe appropriate countermeasures by Identifying threats and vulnerabilities that may compromise assets. (C2, PLO1)
CLO 2: Analyze a range of issues and recommendations pertaining to privacy, surveillance, information misuse and internet services. (C4, PLO2)

**Course Format:**

| **Total Student Learning Time (SLT)** (L = Lecture; T = Tutorial; P = Practical; EL = E-Learning) : | | | | | |
|---|---|---|---|---|---|
| **Learning Hours** | | | | **Independent Learning (hr)** | **Total Student Learning Time (hr)** |
| L | T | P | EL | | |
| 28 | 14 | 0 | 14 | 104 | 160 |

**Teaching and Delivery Methods/ Teaching Methodology:**

Lectures, Tutorial and Practical/Laboratory work delivered in a combination of blended & independent learning

E-Learning provided by INTI makes learning more accessible and convenient for the students. The blended model utilized by INTI is the integration of E-learning via INTI's Learning Management System and the conventional lecturer-led classroom activities. INTI students are required to access to the online learning materials (additional notes, reading materials, online assessments, discussion forums and etc.), so as to acquire a complete learning process. This also promotes self-directed learning in encouraging INTI students to be independent learners.

**Syllabus**:

| Lecture | Course Content Outline | CLO* |
|---|---|---|
| 1-2 | **Overview of Cybersecurity**<br>Aims of cyber security, coupled with contemporar**y threats and vulnerabilities towards computer systems and information assets** | 1 |
| 3-4 | **Internet and network related threats and countermeasures**<br>**Networking and communications**<br>Fundamentals, security challenges, standards | 1,2 |
| 5-7 | **Eavesdropping**<br>surveillance and privacy infringing techniques and technologies | 1,2 |
| 8-10 | **Information protection through risk management, access control and classification** Managing security risks: risk analysis and management | 1,2 |
| 11-13 | **Malware**<br>Types of malware, Attack vectors, Preventing infection Virus and Worm, Sniffing 1. Introduction to viruses, Stages and types of viruses, Virus and worm countermeasures, Types of sniffing attacks | 1,2 |
| 14-16 | **Human factors in cyber security**<br>Internal threat, Social Enginerring, Common targets of social engineering, Social engineering countermeasures, Denial of Service, DoS attack tools, detection techniques, countermeasures. | 1,2 |
| 17-19 | **Contemporary cryptographic techniques and technologies**<br>Basics of Cryptography, Public-key Cryptography, Types of Computer Encryption, Digital Signature, Role of Cryptography in Data Security. | 1,2 |
| 20-21 | **Identification, authentication and authorization**<br>access control, passwords, two-factor authentication | 1,2 |
| 22-24 | **Operating system and software security issues, concepts and techniques**<br>O/S basics, Why is O/S hacked? Case study of some O/S Vulnerabilities and Security Issues, upgrades and patches for O/S | 1,2 |
| 25-26 | **Physical security**<br>Mechanisms for protecting computer systems and information assets | 1,2 |
| 27-28 | **Introduction to ethical hacking and hacking stages**<br>What is Ethical Hacking and? Who is an Ethical Hacker? Difference between Penetration Testing and Ethical Hacking, Five stages of hacking stages: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks | 1,2 |
| | Final Examination | |

**Student Evaluation:**

| **Continuous Assessment** | | **Percentage (%)** | **CLO** |
|---|---|---|---|
| 1 | Test | 20 | 1 |
| 2 | Assignment | 20 | 2 |
| 3 | Project | 20 | 2 |
| **Final Assessment** | | **Percentage (%)** | |
| Final Examination | | 40 | 1 |
| **Total** | | **100%** | |

**Final exam format**:
Section A: 20 Multiple Choice Questions (40 marks). Students must answer ALL questions.
Section B: Essay Questions (60 marks). Answer THREE essay questions. All questions carry equal marks.

**Grading Scale:**
A+ (90-100), A (80-89), A- (75-79), B+ (70-74), B (65-69), B- (60-64), C+ (55-59), C (50-54), C- (45-49), D (40-44), F (0-39), Resit Pass, RP (50-100), Resit Fail, RF (0-49)

**IMPORTANT NOTE:**
Students are required to "**PASS**" BOTH continuous and final assessment in order to pass the subject.

**Additional Information:** NIL

**Main Reference(s) Supporting Course:**

1. Chuck Easttom (2020) Computer Security Fundamentals Fourth Edition (Pearson IT Cybersecurity Curriculum (ITCC)) 4th Edition.

**Additional References:**

1. Yuri Diogenes & Erdal Ozkaya (2018) Cybersecurity – Attack and defense strategies: Infrastructure security with Red Team and Blue Team tactics, 1st Edition, Packt Publishing