Module code	TF-4307		
Module Title	Information Communication Security		
Degree/Diploma	Bachelor of Engineering (Information Communication Systems)		
Type of Module	Major Option		
Modular Credits	2	**Total student workload**	4 hours/week
		Contact hours	2 hours/week
Prerequisite	None		
Anti-requisite	SS-4310 Computer Security		

Aims

This module introduces the different elements that need to be considered in maintaining and securing communication network. It includes network security, security and risk management as well as asset security. Also included are access control, identity management, and cryptography.

Learning Outcomes:

On successful completion of this module, a student will be expected to be able to:

Lower order :	40%	- comprehend the procedure for risk assessment and its relationship with the development of policies, standard and guidelines - comprehend cryptographic concepts and explain its role in different applications
Middle order :	40%	- analyse different network configurations, identify threat and vulnerabilities - implement appropriate authentication, authorisation and access control to satisfy different requirements - analyse different methods to mitigate identified application, data and host security risks
Higher order:	20%	- interpret analysis result, recommend appropriate security improvements and communicate result - design network elements and controls to fulfil given communication requirement

Module Contents

- General security requirement, risk management and the development of policies, standard and guidelines
- Common attacks (malware, social engineering, application attacks) and tools to identify and mitigate against the attacks
- Different network devices (firewalls, routers, load balancers, UTM security appliances, etc.) and components (DMZ, Virtualisation, sub-netting etc.) and its usage in different network architecture design
- Application, data and host securities – identification, tools and techniques
- Access control, authentication, authorization and identity management as well as the different services available
- General cryptography concepts and its applications (Symmetric vs. Asymmetric encryption, hash algorithm)

Assessment	Formative assessment	Monthly online multiple choice and file upload questions will be used to evaluate their learning
	Summative assessment	Examination: 60%
		Coursework: 40% - 2 class tests (10% each) - 2 individual laboratory assignments (10% each)