1.	**Course Title**	**Computer & Information Security**		
2.	**Course Code**	**CSEC3513**		
3.	**Status**	Faculty		
4.	**Credit Hour**	Credit hour: 3 (2+1) 2 for lecture (2 hours per week x 14 weeks) 1 for tutorial (1.5 hours per week x 14 weeks) Lab works-using simulator & emulator supervised by tutor		
5.	**Semester/Year**	1/3		
6.	**Prerequisites**	CCPS1513 Computer Programming		
7.	**Teaching method:**	Distance Learning (Electronic)		
8.	**Evaluation**	**Assessment and Marking Percentage:** Participation 5% Quizzes 15% Project 15% Mid Sem Exam 15% Final Examination 50%		
9.	**Lecturer**			
10.	**Objective of the Subject**	To introduce the different security threats in computing environment and the solutions.		
11.	**Learning Outcomes**	By the end of the subject, students should be able to • Describe and interpret the Fundamental of Computer Security. • Identify the potential threats and security issues in stand-alone network and database computing environment. • Describe and interpret the Fundamentals of Networking and Telecommunication Security. • Identify the legal understanding issues on Computer Security, Software Violation and computer based Security Standards.		
12.	**Synopsis**	The major area of this course includes: Potential threats such as Viruses, Worms, Basics of cryptography, encryption algorithms, Network security, database security and legal issues.		
13.	**Topics**	Details	Lecture (Hrs)	Tutorial (Hrs)
	Topic 1	**1. Fundamental of Computer Security** Objectives, privacy and Ethics, Risk Analysis in computer security, Threats and security, security measures, physical protection (natural disaster, Physical facility, Access Control, Hardware and Software Security Control, Viruses (Trojan Horses, Worms and Logic Bomb), Encryption and Cryptography Techniques.	8	6
	Topic 2	**2. Developing Secure Computer Systems** External Security Measures, Issue, Security Models (Specification and Verification, Bell and LaPadulla Model, Clark-Wilson Model, Goguen-Meseguar, TCSED), Discretionary Access and Information Flow Control, Auditing and Intrusion Detection, Damage Control and Assessment, Microcomputer Security	6	4
	Topic 3	**3. Network and Telecommunication Security** Fundamentals, Issue, Objective and Threats, Security Services, Distributed System Security, The Trusted Network Interpretation, TNI Security Services, AIS Interconnection Issues, Firewalls (Gateway, Application, Cost and Effectiveness)	6	4
	Topic 4	**4. Database Security** Security Requirements to Databases, Designing the Security, Methods of Protection, Security of Multilevel Database	4	3
	Topic 5	**5. Legal Issue and Current Legislation** Computer Crime, Software Violation, Crimes, Privacy Considerations, Corporate Policy, Managerial Issues, Government – based Security Standards, New Techniques and future Plans : Ergonomics	4	3
		Total contact hours	28	21
		Equivalent lecture hours	28	14

		Total lecture hours	42
		Credit hours	3
14.	**Main reference:**	Stalling, W.& Brown, L. (2008) **computer security: principle and practice**. New Jersey: Prentice Hall.	
15.	**Additional References:** **Other Materials:**	1. Conklin, W.A, White, G.B., Cothren, C., Williams, D.,& Davis, R.L.(2005). **Principles of computer security: security + and beyond**. Singapore: McGraw Hill. 2. Merkow, M., & Breithaupt, J. (2006). **Information security principles and practices**. New Jersey:Pearson Prentice Hall. All other materials will be available to students online.	