

DCOMP345 – SECURITY IMPLEMENTATION & MANAGEMENT

MODULE DETAILS

Course Location	: Sierra Leone
Department	: Faculty of Information & Computer Technology
Program Name	: B Sc (Hons) in Information Technology
Credits	: 3
Status	: Major
Contact Hours Per Week	: 3 hours (2 hrs lecture + 1 hr tutorial)
No. of weeks (Contact)	: 12 Teaching Weeks + 1 Final Examination Week + 1 Mid Term Break Week
Teaching Pattern	: Lectures, Tutorials & Presentation
Pre-requisite	: Introduction to Information systems
No. of assignments	: 2
Lecturer's Name	: Gibril Njai
E-mail	: gibril.njai@limkokwingedu.sl

Prepared by : Gibril Njai

Approved by : AQA

Signature : _____ Date _____

Signature : _____ Date _____

Verified by : Oluwatosin Ayorinde

Signature : _____ Date _____



This document comprises the following:

- Essential Information
- Specific Module Information
- Module Rules & Regulations
- Grades
- Plagiarism
- Module Introduction
- Module Aims & Objectives
- Learning Outcome
- Specific Generic Learning Skills
- Syllabus + Lecture Outline
- References
- Assessment Schedule
- Assessment Criteria
- Specific Criteria
- Learning Activities
- Specific Criteria

Other documents as follows will be issued to you on an ongoing basis throughout the semester:

- Handouts for Assignments
- Submission Requirements + Guidelines

1.0 ESSENTIAL INFORMATION

- All modules other than electives are '**significant modules**'
- As an indicator of workload one credit carries and additional 2 hours of self-study per week. For example, a module worth 3 credits require that the student spends an additional 6 hours per week, either reading, completing the assignment or doing self directed research for that module.
- **Submission of ALL assignment work is compulsory in this module, failure to do so a DNS (Did not submit) grade would be awarded. An overall grade of DNC (Did not complete) would be set for those who fail to submit a major piece of assessment work (major assignment i.e.:**

Class Test, Major Assignment + Final examination). A student cannot pass this module without having to submit ALL assignment work by the due date or an approved extension of that date.

- All assignments are to be handed on time on the due date. Students will be penalised 10 percent for the first day and 5 percent per day thereafter for late submission (a weekend or a public holiday counts as one day). Late submission, after the date Board of Studies meeting will not be accepted.
- Due dates, compulsory assignment requirements and submission requirements may only be altered with the consent of the majority of students enrolled in this module at the beginning/early in the program.
- Extensions of time for submission of assignment work may be granted if the application for extension is accompanied by a medical certificate.
- Overseas travel is not an acceptable reason for seeking a change in the examination schedule.
- Only the Head of School can grant approval for extension of submission beyond the assignment deadline.
- Re-submission of work can only receive a 50% maximum pass rate.
- Supplementary exams can only be granted if the level of work is satisfactory **AND** the semester work has been completed.
- Harvard referencing and plagiarism policy will apply on all written assignments.

2.0 SPECIFIC MODULE INFORMATION

- Attendance rate of 80% is mandatory for passing module.
- All grades are subject to attendance and participation.
- Absenteeism at any scheduled presentations will result in zero mark for that presentation.
- Visual presentation work in drawn and model form must be the original work of the student.
- The attached semester program is subject to change at short notice.

3.0 MODULE RULES AND REGULATIONS:

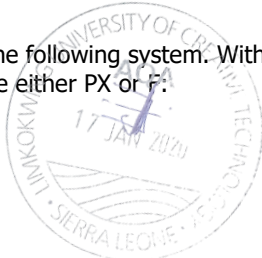
Assessment procedure:

- These rules and regulations are to be read in conjunction with the UNIT AIMS AND OBJECTIVES
- All assignments/projects must be completed and presented for marking by the due date.
- Marks will be deducted for late work and invalid reasons.
- All assignments must be delivered by the student in person to the lecturer concerned. No other lecturer is allowed to accept students' assignments.
- All tests/examinations are compulsory.
- Students must sit the test/examination on the notified date.
- Students are expected to familiarise themselves with the test/examination timetable.
- Students who miss a test/examination will not be allowed to pass.

- Any scheduling of tutorials, both during or after lecture hours, is TOTALLY the responsibility of each student. Appointments are to be proposed, arranged, confirmed, and kept, by each student. Failure to do so in a professional manner may result in penalty of grades. Tutorials WITHOUT appointments will also NOT be entertained.
- Note that every assignment is given an ample time frame for completion. This, together with advanced information pertaining deadlines gives you NO EXCUSE not to submit assignments on time.

4.0 GRADES

All modules and assessable projects will be graded according to the following system. With respect to those units that are designated 'Approved for Pass/Fail' the grade will be either PX or F:



Grade	Numeric Grade	Description
90 – 100	A+	Pass with Distinction
85 – 89	A	
80 – 84	A-	
75 – 79	B+	Pass with Credit
74 – 70	B	
65 – 69	B-	
60 – 64	C+	Pass
55 – 59	C	
50 – 54	C-, PX, PC	
0 – 49	F	Fail

EXP	Exempted
PC	Pass Conceded
PP	Pass Provisional with extra work needed
PX	Pass after extra work is given and passed
X	Ineligible for assessment due to unsatisfactory attendance
D	Deferred
W	Withdraw
DNA	Did Not Attend Module
DNC	Did Not Complete Module

5.0 PLAGIARISM, COPYRIGHT, PATENTS, OWNERSHIP OF WORK: STUDENT MAJOR PROJECT, THESES & WORKS

See LIMKOKWING, HIGH FLYERS HANDOUT, pg 10.

6.0 MODULE INTRODUCTION

This module will introduce students the security implementation and management, and presents solutions that can be integrated in many different phases in the security systems development life cycle. The module provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents and designing a consistent, reasonable information security system with appropriate intrusion detection and reporting features.

7.0 MODULE AIMS AND OBJECTIVES

This module will expose students to the spectrum of security activities, methods, methodologies and procedures. They will also be exposed to the inspection and protection of information assets, detection of and reaction to threats to information assets, integration of confidentiality, integrity, authentication and availability into system development and examination of pre and post incident procedures, technical and managerial.

8.0 LEARNING OUTCOME

The students will be expected to:

- Understand the key terms and critical concepts of information security
- Outline the phases of security systems development life cycle
- Understand the roles of professional involved in information security within an organization.



9.0 UNIT SYLLABUS + LECTURE OUTLINE:

Week:	1
CHAPTER 1:	INTRODUCTION TO SCURITY IMPLEMENTATION AND MANAGEMENT
<i>Lecture Synopsis:</i>	<ul style="list-style-type: none">1.1 Overview of Information Security1.2 Key Terms of Information Security1.3 Critical characteristics of Information1.4 NSTISS Security Model1.5 Spheres of Security1.6 Components of Information security1.7 Securing the components1.8 Balancing Security and access1.9 Approaches to security implementation

Week:	2. WHY WE NEED SECURITY
CHAPTER 2:	<ul style="list-style-type: none">2.1 The Systems development Life Cycle2.2 The Security Systems development Life Cycle2.3 System vulnerability analysis, threats analysis, and attacks.2.4 Threat Matrix2.5 Software Development Security Problems2.6 Attack Replication Vectors

Handout: *Tutorial 1, Individual Assignment*

Week: 3
CHAPTER 3: THE LEGAL, ETHICAL & PROFESSIONAL ISSUES IN INFORMATION SECURITY

Lecture Synopsis:

- 3.1 Theory of Technology Law and Ethics in Information Security
- 3.2 Types of Laws
- 3.3 International Laws and Legal Bodies
- 3.4 Policy Versus Law
- 3.5 Ethical Concepts in Information Security
- 3.6 Codes of Ethics, Certifications, and Professional Organizations
- 3.7 Organizational Liability and the Need for Council

Handout: Tutorial 2

Week: 4
CHAPTER 4: RISK MANAGEMENT

Lecture Synopsis:

- 4.1 Overview of Risk Management,
- 4.2 Component of Risk Management
- 4.3 Risk Control Strategy
- 4.4 Selecting a Risk Control Strategy
- 4.5 Risk Control Cycle
- 4.5 Cost Benefit Analysis (CBA)

Handout: Tutorial 3
Due date: Individual Assignment

Week: 5
CHAPTER 5: PLANNING FOR SECURITY

Lecture Synopsis:

- 5.1 Continuity Strategy
- 5.2 Business Impact Analysis
- 5.3 Incident Response Planning
- 5.4 Incident Reaction
- 5.5 Incident Recovery
- 5.6 Automated Response
- 5.7 Business Continuity Planning
- 5.8 Model for a Consolidated Contingency Plan

Handout: Tutorial 4

Week: 6 & 7
CHAPTER 6: SECURITY TECHNOLOGY; IDS, ACCESS CONTROL, FIREWALLS, VPNs AND OTHER SECURITY TOOLS

Lecture Synopsis:

- 6.1 Physical Design of the SecSDLC
- 6.2 Firewalls
- 6.3 Dial-up Protection
- 6.4 Intrusion Detection Systems (IDS)
- 6.5 Scanning Analysis Tools
- 6.6 Content Filters
- 6.7 Trap and Trace
- 6.8 Access Control Devices
- 6.9 Protecting Remote Connections

Handout: Tutorial 5, Major Assignment

Week 7: Class Test

Week: 8
SEMESTER BREAK

Week: 9
CHAPTER 7: CRYPTOGRAPHY AND PHYSICAL SECURITY
Lecture Synopsis: 9.1 Cryptography, Terminology and Encryption-based Solutions
9.2 Cipher Methods
9.3 Cryptographic algorithms
9.4 Cryptographic Tools
9.5 Some protocol for secure communication
9.3 Attacks on cryptosystems

Handout: Tutorial 6

Week: 10
CHAPTER 8: IMPLEMENTING SECURITY
Lecture Synopsis: 10.1 Project Management
10.2 Technical Topics of implementation
10.3 Nontechnical Topics of Implementation

Handout: Tutorial 7

Week: 11
CHAPTER 9: INFORMATION SECURITY MANAGEMENT
Lecture Synopsis: 11.1 Managing for Change
11.2 Security Management Models
11.3 The Maintenance Models
11.4 Security Management
11.5 Advanced Security and beyond

Handout: Tutorial 8

Week: 12
CHAPTER 9: PERSONNEL SECURITY
Lecture Synopsis: 12.1 Security Function within an Organization's Structure
12.2 Staffing the Security Function
12.3 Credentials of Information Security Professionals
12.4 Employment Policies and Practices
12.5 Security Consideration of Nonemployees

Handout: Tutorial 9

Due date: Major Assignment

Week: 13
Major Project Presentation

Week: 14
Revision

Week: 15 & 16
FINAL EXAMINATION WEEK

11.0 REFERENCES

1. Michael E. Whitman and Herbert J. Mattord, *Management of Information Security*, 3rd Edition
2. Charles P. Pfleeger, & Shari Lawrence Pfleeger, *Security in Computing*, 3rd Edition, ISBN: 0-13-035548-8
3. Mark Ciampa, Thomson Course Technology, *Security + Guide to Network Security Fundamentals, Thomson Course Technology*, ISBN: 0-619-21566-6
4. William Stallings, *Network Security Essential, Application and Standards*, 3rd Edition, ISBN: 0132380331

12.0 ASSESSMENT SCHEDULE

ASSESSMENT	Issue Date	Due Date	%
Assignment 1	week 2	week 4	15
Mid Semester Test	week 7	week 7	20
Major Project	week 6	week 12	25
FINAL EXAMINATION	week 15	week 16	40
TOTAL			100

13.0 ASSESSMENT CRITERIA

Process of grading and criteria used to determine the grades, passes and high distinctions.

14.0 SPECIFIC CRITERIA

- Each assignment will be handed out with the project brief and will vary, depending on the teaching and learning objectives of the specific assignment.