Module 3: Managing Information Security

Stage				1			
Semester				1			
Module Title				Managing Information Security			
Module Number				3			
Module Status				Mandatory			
Module ECTS Credits				10			
Module NFQ level				9			
Pre-Requisite Module Titles				None			
Co-Requisite Module Titles				None			
Capstone Module?				No			
List of Module Teaching Personnel				Mr Alan Hannaway			
Contact Hours				**Non-contact Hours**			**Total Effort (hours)**
60				**140**			**200**
Lecture	**Practical**	**Tutorial**	**Seminar**	**Assignment**	**Placement**	**Independent Work**	
36		24		40		100	
Allocation of Marks (Within the Module)							
	Continuous Assessment	**Project**	**Practical**	**Final Examination**			**Total**
Percentage Contribution	**40**			**60**			**100**

Intended Module Learning Outcomes

On successful completion of this module learners will be able to:

1. Discuss modern security: systems, networks, multi-user systems, connections, mechanisms, devices and procedures.
2. Critically comment on the roles in organisations with regard to Information Security.
3. Demonstrate awareness and critical understanding of Asset Management, Data Classification, Audit and Governance and the environment within which they operate.
4. Evaluate the threat that software and operating systems face in achieving information security
5. Critically analyse insecurity in software, and document measures to address risks identified

Module Objectives

This module aims to give the learner an understanding of the issues relating to the management of information security in modern industry. It explores the roles, policies and procedure applied in information security. The module further explores the specific role that software systems play in the threat against information security.

Module Curriculum

- **What is Security?**
  Concepts of information security
  Security Models
  Principles of Information security management

- **Planning for Security**
  The role of planning
  Strategic planning
  Information Security Governance
  Planning for contingencies

- **Information Security Policy**
  Policy, Standards and practices
  Levels of security, Enterprise, System, Issue specific
  Guidelines for effective policy

- **Organising for Security**
  The place of information within the organisation
  Elements of a Security Programme
  Security Roles and Titles
  Training and Awareness of Security

- **Models of Security Management**
  Access Control
  Security Architectures
  Security Management Models

- **Security Management Practices**
  Benchmarking
  Performance measures
  Certification and Accreditation

- **Software Flaws and Malware**
  Introduction to the concepts of software flaws
  Malware and botnets
  Miscellaneous software-based attacks

- **Operating systems and security**
  Operating system security functions
  The concepts of a trusted operating systems

Next generation secure computing bases

Reading lists and other learning materials

Recommended reading

Whitman M., Mattord H., 2010, *Management of Information Security 3rd Edition,* Course Technology

Stamp M, 2011*, Information Security: Principles and Practice 2nd Edition*, Wiley

Secondary reading

Ward Bynum T., Rogerson S., 2004, *Computer Ethics and Professional Responsibility*, Blackwell

Lacey D., 2009, *Managing the Human Factor in Information Security: How to win over Staff and Influence Business Managers,* Wiley & Sons

Module Learning Environment

Accommodation

Lectures are carried out in class rooms / lecture halls in the College. Lab tutorials are carried out in computer labs across the Campus. There is also a dedicated hardware lab.

Library

All learners have access to an extensive range of physical and electronic (remotely accessible) library resources. The library monitors and updates its resources on an on-going basis, in line with the College's Library Acquisition Policy. Lecturers update reading lists for this course on an annual basis as is the norm with all courses run by Griffith College.

Module Teaching and Learning Strategy

The module is taught using a combination of lectures and tutorials. The learners are expected to engage in research of security issues in a modern environment and critically evaluate policies and strategies.

Module Assessment Strategy

Element No	Weighting	Type	Description	Learning Outcome Assessed
1	20%	Essay	Write an essay dealing with a real world security management issue involving practical research.	1, 2, 3
2	20%	Report	Write a report based on a case study of a real world software insecurity problem. The learner will analyse the problem and make recommendations to the company based on the analysis.	3, 4, 5
3	60%	Examination	End of module examination	1, 2, 3