Module 7: Legal and Ethical Aspects of Information Security

Stage				1			
Semester				2			
Module Title				Legal and Ethical Aspects of Information Security			
Module Number				7			
Module Status				Mandatory			
Module ECTS Credits				5			
Module NFQ level				9			
Pre-Requisite Module Titles				None			
Co-Requisite Module Titles				None			
Capstone Module				No			
List of Module Teaching Personnel				Dr Faheem Bukhatwa Guest Lecturers			
Contact Hours				**Non-contact Hours**			**Total Effort (hours)**
36				**64**			**100**
Lecture	**Practical**	**Tutorial**	**Seminar**	**Assignment**	**Placement**	**Independent Work**	
24			12	30		34	
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 the learner will be able to:

1. Demonstrate an awareness and critical appreciation of the importance of information security from legal and ethical perspectives
2. Discuss the legal and ethical responsibilities and obligations relating to information security
3. Explain the origin and development of Irish and International law on information security
4. Analyse and document the legal requirements relating to collection, storing and maintaining, supplying and securing information
5. Demonstrate understanding of the information and material required for evidence.

Module Objectives

This module aims to provide the learner with the knowledge and understanding of the legal and ethical issues surrounding information and information security, privacy and data protection. The module gives the learner an understanding of Irish and international information relating laws. The learner also focusses on the legal and ethical aspects of computer crimes and their investigations, and issues relating to intellectual property. The module does not aim at have the learner becoming an expert in legal matters but will make the learner aware of legal responsibilities and be able to recognise when a lawyer is required.

Module Curriculum

- **Information Security: Legal and Ethical Perspectives**
  Information security: definition, objectives and controls from legal and ethical perspectives
  Legal response to security: declaring conduct illegal, requiring the protection of data
  Legal and ethical duty to provide security against internal and external threats
  Understanding responsibility and obligation

- **Information Security Laws**
  Origin and evaluation of information security laws
  Challenges of access to information, hacking, data protection, privacy and piracy in a networked world

- **Reporting, Investigations and engaging with internal and external bodies**
  Role of statutory bodies and law enforcement agencies in implementing the laws
  Identifying and reporting an information security breach both from legal and ethical perspective
  Working with internal investigating committees and external statutory & law enforcement agencies in case of security breach

- **Assessing and monitoring policies and controls from legal and ethical perspective**
  Assessing organisational information system security controls
  Information Security Risk Assessment from legal and ethical perspective
  Reviewing and analysing organisational information security plans from legal and ethical perspective

Recommended Reading

Whitman M E, Mattford H J, 2010, *Readings and Cases in Information Security: Law and Ethics*, Delmare Cengage Learning

Smedinghoff T J, 2008, *Information Security Law: The Emerging Standard for Corporate Compliance*, IT Governance

Secondary Reading

Salehnia A, 2002, *Ethical Issues of Information Security*, IGI Press

Additional reading material will include peer reviewed research papers and most recent and relevant case studies.

Module Learning Environment

Accommodation

Lectures are carried out in class rooms / lecture halls in the College. Computer Labs throughout the Campus are accessible for the purpose of completing assignments. There is no specific software required to deliver the programme.

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 seminars. Lectures are used to explain the concepts, and seminars are used to develop and discuss information presented in lectures. It is intended that a number of seminars will be delivered by guest lecturers. Some seminars involve the discussion of seminal research papers and case studies in the domain of legal and ethical aspects of information security. Learners are expected to read the material prior to seminars.

Module Assessment Strategy

Element No.	Weighting	Type	Description	Learning Outcomes Assessed
1.	15%	Report	Write a critical report on a case study assigned by the lecturer	1,2
2.	25%	Research Paper	A research paper on a real world security incident; this should be an original piece of research.	3,4
3.	60%	Closed Book Examination	End of Module Examination	All