MODULE DESCRIPTOR

MODULE TITLE	Electronic Crime		
Module Code	44-6981-00L/S		
Level	6		
Credit Points	20		
Indicative Assessment Components & Percentage Weightings	Coursework 75% Exam 25%		
Pre-Requisite Modules ***(if applicable)***			
Delivered according to Standard Academic Calendar YES / NO	**Long:** **2 semesters** YES	**Short:** **1 semester** NO	**Other delivery pattern:** *Please specify*

1 MODULE AIMS

Information and Communication Technology (ICT) is a pervasive force in today's society, it provides global access to information, new and innovative ways of doing business, a vehicle for education and recreation and much more. Unfortunately ICT and the Internet in particular is also a target of diverse and extensive abuse and attacks. As increasing numbers of individuals and businesses connect to the Internet it is essential that undergraduates are not only aware of the threats and vulnerabilities associated with the use of ICT, but they are also aware of the responses to these threats and vulnerabilities.

The aims of this module are to:

- identify the threats and vulnerabilities existing within ICT;
- help students understand and assess the impact of the major types of commonly encountered electronic crime; and
- review and assess the protection and assurances available to individuals and business to avoid becoming victims of electronic crime.

2 MODULE LEARNING OUTCOMES
BY THE END OF THE MODULE YOU WILL BE ABLE TO:

1. Assess the vulnerabilities within contemporary Information Systems;
2. Identify and assess the threats posed by the major types of commonly-encountered electronic crime;
3. Critically evaluate the current legislation that exists to protect individuals and businesses from electronic crime;
4. Present discursively risk management processes necessary for ICT;

5. Critically evaluate the best practice in IT security by a consideration of IT governance remedies offered through a variety of codes of practice and standards;

6. Assess and evaluate each of the stages in forensic computing - the acquisition, authentication and preservation, and analysis of electronic evidence;

7. Evaluate the major software applications used in forensic computing;

8. Assess the role of the expert witness in forensic computing.

3 INDICATIVE LEARNING, TEACHING AND ASSESSMENT ACTIVITIES

The module will be delivered by a series of lectures and small group seminars. The lectures will deliver the core material of the module.

The small group seminars will be student centred and will be based on discussions, case studies and analysis of topical cases; the seminars will explore topical issues related to the core material of the module.

A series of student led presentations based on research into key topics will be a main feature of the small group seminars.

Feedback will be provided throughout the module. Formative feedback will be given during the small group seminars. Oral feedback will be given on preparatory work for student led presentations and at the completion of the presentation. Written feedback will be provided for the presentations (this will be based on the oral feedback provided at the time of the presentation) and also on completion of the essay. It is expected that students will act on the feedback given.

Assessment will take the form of coursework (e.g. group presentation and essay) and examination.

ASSESSMENT STRATEGY AND METHODS

Task No.	TASK DESCRIPTION	SI Code	Task Weighting %	Word Count / Duration	In-module retrieval available
1	Coursework	CW	75%	3500 words	No
2	Exam	EX	25%	1 hour	No

4 INDICATIVE MODULE CONTENTS / TOPICS

- Vulnerabilities of and threats to, Information Systems within organisations, the commercial use of the Internet, IT infrastructure;
- History and developments of electronic crime, e g malware, denial of service and distributed denial of service, hacking, spyware;
- Frameworks for classifying electronic crime;
- Legislation, Computer Misuse Act and associated cases, other relevant legislation; International comparison of legislation;
- Government and commercial initiatives for IT governance and IT security;
- Forensic Computing and Electronic evidence; and
- Software applications for forensic computing.

FURTHER INFORMATION ABOUT THIS MODULE

FURTHER ADDITIONAL INFORMATION IS AVAILABLE TO SUPPORT THIS MODULE, INCLUDING ASSESSMENT CRITERIA DETAILING HOW YOUR PERFORMANCE IN THE MODULE WILL BE MEASURED, HOW YOU WILL RECEIVE FEEDBACK, DETAILS OF LEARNING RESOURCES AND KEY READINGS.

THIS INFORMATION CAN BE FOUND IN THE MODULE HANDBOOK AND FROM THE MODULE ON-LINE SITE.

NOTE THAT THIS ADDITIONAL INFORMATION MAY BE SUBJECT TO CHANGE FROM YEAR TO YEAR.

FINAL TASK

According to the Assessment Strategy shown in the Module Descriptor, which task will be the LAST TASK to be taken or handed-in? (Give task number as shown in the Assessment Strategy)	Task No. 2

MODULE REFERRAL STRATEGY

Task for Task (as shown for initial assessment strategy)	Y
Single Referral Package for All Referred Students	N

REVISIONS

Date	Reason
July 2012	Assessment Framework review