MODULE SPECIFICATION

Part 1: Information			
Module Title	Computer Security		
Module Code	UFCFHE-30-3	Level	Level 6
For implementation from	2018-19		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Contributes towards			
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Educational Aims: See Learning Outcomes

Outline Syllabus: Software Security in the real world: analysing systems and security aware applications from various domains such as mobile communications, electronic commerce, banking and finance.

Trusted computing and trust in electronic commerce and the existence of a trusted computing base.

Policies for managing security, policy languages and models.

Trust and Reputation and the basis for authorization decisions; the notion of trust and how to express it (subjective logic, trust and uncertainty, rating systems and reputations servers); the eBay reputation server as an example; communities of trust.

Security analysis; assumptions made, social basis and threat assumptions. Trade off between

threats and countermeasures and the return on security investment (RoSI).

Information Security Management Standards and Codes of Practice. Legislation. The interrelation and interdependency of security management and other system management activities and considerations such as:- Business continuity management, organisational security, asset classification and control, personnel security, physical and environmental security, communications and operations management, systems development and maintenance, business continuity management and compliance.

Teaching and Learning Methods: 108 hours scheduled learning

192 hours for independent research and assessment preparation.

Scheduled learning will typically include lectures, seminars, supervision and an interactive forum.

All students are expected to attend a series of tutorials.

Introductory lectures are supported by seminars, case studies, visits and practical workshops. In addition this module will be supported by interactive forums and learning tools.

300 hours study time of which 108 hours will represent scheduled learning.

Independent learning includes hours engaged with essential reading, case study preparation, assignment preparation and completion. Student study time will be organised each week with a series of both essential and further readings and preparation for practical workshops.

This unit takes a broad view of computer security within an organisational context, addressing hardware, software and management related issues that require both a reactive and proactive approach to ensure business continuity. A practical approach will be used to the develop the tools and techniques for the effective implementation of computer security within a commercial environment.

Part 3: Assessment

A range of assessment techniques will be employed to ensure that learners can meet the breadth of learning outcomes presented in this module alongside the ability to demonstrate transferable skills e.g. communication skills.

Exam: Security tools and techniques.

Reflective research essay: Students will be expected to analyse a given scenario, identify security issues and make suitable recommendations for enhance the measures in place in order to ensure business continuity.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Written Assignment - Component B	✓	50 %	Reflective research essay (2500 words)
Examination - Component A		50 %	Unseen Exam (2 hours)
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Written Assignment - Component B	✓	50 %	Reflective research essay (2500 words)
Examination - Component A		50 %	Unseen Exam (2 hours)

Part 4: Teaching and Learning Methods

Learning Outcomes

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

	Module Learning Outcomes
MO1	Demonstrate analysis of the motivations leading to malicious behaviour
MO2	Identify and evaluate a range of real world security issues faced by commercial organisations
MO3	Devise appropriate management strategies and procedures to counter threats
MO4	Appraise the usefulness of a range of security techniques for dealing with particular situations
MO5	Assess security risks and produce a security policy
MO6	Evaluate the goals and techniques of effective organization and implementation of information security
MO7	Critically appraise the significance of UK security laws, regulations and standards in relation to global issues
MO8	Identify the components required for a successful disaster recovery process

Contact Hours

Contact Hours	
Independent Study Hours:	
Independent study/self-guided study	192
Total Independent Study Hours:	192
Scheduled Learning and Teaching Hours:	
Face-to-face learning	108
Total Scheduled Learning and Teaching Hours:	108
Hours to be allocated	300
Allocated Hours	300

Reading List

The reading list for this module can be accessed via the following link:

https://uwe.rl.talis.com/index.html