MODULE SPECIFICATION

Part 1: Information			
Module Title	Information Security		
Module Code	UFCFHJ-15-M	Level	Level 7
For implementation from	2020-21		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
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: Foundational: information security principles, information risk; threats and vulnerabilities

Key information security issues: regulation; privacy; civil liberties; intellectual property and cybercrime

Information security management: ethics; frameworks and policies; secure software development; physical and environmental security; disaster recovery and business continuity management

Technical information security controls: authentication and authorisation; data security; network security; computer security; application security

Information security trends: governance; identity and access management; mobile and cloud security

Teaching and Learning Methods: The core module content is introduced through lectures. All teaching and learning activities (both scheduled and independent) are aligned with the learning outcomes. Tutorials and seminars aim to reinforce and extend the material delivered in the lectures.

Independent learning requires students to spend time in directed reading, developing research skills and in collaboration with other students in order to assimilate material presented during the contact hours to develop this further for the group assignment.

This 15 credit module requires (notionally) 150 hours of study. The module delivery is organised as follows:

Contact time: 25% for lectures, tutorials, seminars and tutor-led activities: 24 hours.
Assimilation and development of knowledge: 50% for independent learning, both individually and within groups: 86 hours.
Assessment: 25% examination and 75% coursework: 40 hours, which approximately equates to:
Exam preparation approximately 6% (10 hours): reviewing selected module content against examined learning outcomes.
Coursework preparation approximately 19% (30 hours): preparing group coursework for assessment.
Total study time: 150 hours.

The teaching and learning strategy enabling the examination is:
Scheduled learning:
Lectures – introduces topics (relevant to learning outcomes 1 and 4) to be assessed.
Tutorials/Seminars – tutor-led teaching and learning activities to deepen the topic(s) covered.

Independent learning:
Directed reading – self-managed study to review and deepen directed topics.
Group collaboration – student-student interaction to elaborate, reflect and apply topics.

Examination preparation:
Tutor guidance – revision session/advice.
Self-directed review of topics addressing learning outcomes 1 and 4, as covered during lectures.

The teaching and learning strategy enabling the group assignment is:
Scheduled learning:
Lectures – introduce some topics (relevant to learning outcomes 2, 3 and 5) that may be chosen by the group for use in the assessment.
Tutorials/Seminars – tutor-led teaching and learning activities to extend and deepen the topic(s) covered. Formative feedback is offered.

Independent learning:
Directed reading – self-managed study to review, deepen and extend directed topics knowledge and understanding.
Group collaboration – student-student interaction to research, elaborate, reflect and apply group chosen topics.

Assignment preparation:
Tutor guidance – group assignment advice.
Self-directed group review of assignment against learning outcomes 2, 3 and 5.

Part 3: Assessment

The assessment strategy has been selected to enable students to demonstrate a rich understanding of the facets of information security and the correct selection and application of controls across a range of contexts (assessed via exam). Credit will be given for students who illustrate wider reading and understanding through the selection of appropriate examples and case studies.

Secondly, through a group assignment, students will develop the ability to work in a team to analyse trends and legislative environment and develop standards-compliant policies – the results of which can be communicated professionally at senior management level in written form, suitably structured and annotated.

Examination (25%)
Learning outcomes 1 (explaining key information security risk, threats etc) and 4 (outlining technical controls) are assessed by a short-answer, controlled-conditions, 1.5 hour examination.

Group Assignment (75%)
Learning outcomes 2 (analysing privacy, civil liberties and intellectual property), 3 (proposing standards–compliant framework/policy) and 5 (collaborating to critique information security trends) are assessed by a group coursework.

Two key dimensions of the group assignment will be assessed:
The product produced by the group.
The group collaboration process, including the skills and effort put in by members of the group in creating the product.

The product will be marked using detailed assessment criteria (published within the assignment brief).

The collaboration process will use distinct assessment criteria. This will apply peer assessment of the group collaboration process to create an individual process weighting factor.

The individual weighting factor will determine the proportion of the product mark awarded to an individual student.

Students will be instructed to adopt UWE advice and policies on study skills, Harvard Referencing and word count.

The assignment length will be around 3,000 words.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Examination (Online) - Component A	✓	25 %	Online Unseen examination (1.5 hours) 24 hour window
Report - Component B		75 %	Group assignment – product report (3,000 words)
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Examination (Online) - Component A	✓	25 %	Online Unseen examination (1.5 hours) 24 hour window
Report - Component B		75 %	Individual report (3,000 words)

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will achieve the following learning outcomes:

Module Learning Outcomes	**Reference**
Synthesise and evaluate key information security principles, risks, threats and vulnerabilities faced by public or private organisations	MO1
Analyse information security issues related to privacy, civil liberties and intellectual property, reporting at board level	MO2
Propose a standards compliant information security framework and/or policy suited for consideration by a public or private organisation board	MO3

	Apply a recognised information security standard to prescribe technical controls appropriate for a public or private organisation	MO4
	Collaborate as a team to research and communicate a critique of current/emerging information security trends to technical and non-technical audiences	MO5
Contact Hours	**Independent Study Hours:**	
	Independent study/self-guided study	126
	Total Independent Study Hours:	126
	Scheduled Learning and Teaching Hours:	
	Face-to-face learning	24
	Total Scheduled Learning and Teaching Hours:	24
	Hours to be allocated	150
	Allocated Hours	150
Reading List	*The reading list for this module can be accessed via the following link:* https://uwe.rl.talis.com/modules/ufcfhj-15-m.html	

Part 5: Contributes Towards

This module contributes towards the following programmes of study:

Information Technology [Jan][FT][Villa][1yr] MSc 2020-21

Information Technology [May][FT][Villa][1yr] MSc 2020-21

Information Technology [Sep][FT][Frenchay][1yr] MSc 2020-21

Information Technology [Sep][FT][Villa][1yr] MSc 2020-21

Information Technology [Sep][PT][Frenchay][2yrs] MSc 2019-20