MODULE SPECIFICATION

Part 1: Information			
Module Title	Business Security		
Module Code	UFCFSM-15-1	Level	Level 4
For implementation from	2018-19		
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		
Contributes towards			
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Educational Aims: This topic provides apprentices with an introduction to the fundamental principles of Information Technology Security and Risk Management at the organisational level. They will learn critical information and cyber security principles and management. The apprentices will address the role of hardware, software, processes, communications, applications, people and policies and procedures with respect to organisational information security.

Outline Syllabus: Develop and complete a security risk assessment

Security threats and hazards to information systems or services e.g. Cloud services

Concepts of threat, hazard and vulnerability

What risk is and how risks are usually characterised (likelihood and impact)

Commonly used risk tools e.g. a risk register

Inherent asymmetric nature of cyber security threats

Capability, opportunity & motive of threats, reflecting on typical hazards and example security objectives

Common vulnerabilities in computer networks and systems e.g. un-secure coding and unprotected networks

Assurance concepts i.e. difference between 'trusted' and 'trustworthy' and explain what assurance is for information security

Main approaches to assurance i.e. intrinsic, extrinsic, design & implementation, operational policy and process, giving examples of how these might be applied at different stages in the lifecycle of a system.

Technical and administrative mitigation approaches

Security models

Teaching and Learning Methods: 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.

150 hours study time of which 36 hours will represent scheduled learning. Scheduled learning includes lectures, seminars, tutorials, demonstration, practical classes and workshops; external visits; supervised time in studio/workshops.

Independent learning includes hours engaged with essential reading, case study preparation, assignment preparation and completion. Apprentice study time will be organised each week with a series of both essential and further readings and preparation for practical workshops. It is suggested that preparation for lectures, practical workshops, session delivery and seminars will take 7 hours per week.

Scheduled learning will typically include lectures, seminars, supervision, external visits and All apprentices are expected to attend a series of tutorials.

Part 3: Assessment

This module is assessed by a combination of techniques: a presentation (30 minutes) and an e-portfolio.

Assessment 1: Presentation (Component A)

Apprentices will carry out a 30-minute research based presentation that discusses core cyber security theory. Apprentices are expected to demonstrate understanding of the concepts of threats, hazards and vulnerability, inherent asymmetric nature of cyber security, technical and administrative mitigation approaches, and the need for a comprehensive security model. It is expected that apprentices will demonstrate wide reading, professionalism, strong communication skills (both verbal and written) as well as effective organisational/time management skills.

Assessment 2: E-Portfolio (Component B)

Apprentices are expected to produce a small e-portfolio, demonstrating basic technical skills in cyber security. This will include core skills such as; creating (for a simple system) a security risk assessment, undertaking a security risk assessment, and proposing basic advice on remedies/preventive measures. Apprentices will also need to analyse and evaluate security threats and hazards to planned and installed information systems or services.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Portfolio - Component B	✓	40 %	E-portfolio
Presentation - Component A		60 %	Presentation (in-class) (30 minutes)
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Portfolio - Component B	✓	40 %	E-portfolio
Presentation - Component A		60 %	Presentation (in-class) (30 minutes)

Part 4: Teaching and Learning Methods

Learning Outcomes

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

	Module Learning Outcomes
MO1	Explain how the concepts of threat, hazard and vulnerability relate to each other and lead to risk
MO2	Explain the inherent asymmetric nature of cyber security threats
MO3	Describe and characterise examples of threats, describing some typical hazards. that may concern an organisation
MO4	Describe some common vulnerabilities in computer networks and systems, and assurance concepts
MO5	Explain technical and administrative mitigation approaches
MO6	Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO)
MO7	Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice
MO8	Analyse and evaluate security threats and hazards to planned and installed information systems or services

Contact Hours

Contact Hours	
Independent Study Hours:	
Independent study/self-guided study	114
Total Independent Study Hours:	114
Scheduled Learning and Teaching Hours:	
Face-to-face learning	36

	Total Scheduled Learning and Teaching Hours:	36
	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/index.html	