MODULE SPECIFICATION

Part 1: Information			
Module Title	Information management and security		
Module Code	UFCFKU-30-2	Level	Level 5
For implementation from	2021-22		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	
Department	FET Dept of Computer Sci & Creative Tech		
Module Type:	Standard		

Pre-requisites	None
Excluded Combinations	None
Co-requisites	None
Module Entry Requirements	None
PSRB Requirements	None

Part 2: Description

Overview: Information security is concerned with protecting an organisations' electronic or physical data. It should protect the confidentiality, availability and integrity of data.

This module is concerned with the way in which electronic data is handled within the organisation, how it is made available, manipulated and analysed. It then examines how management systems are employed to minimise risk without impacting business productivity.

Educational Aims: This module contributes cyber management knowledge and understanding.

Outline Syllabus: You will cover

information management concepts, e.g.:

information storage and retrieval;

information capture and representation;

searching, retrieving, linking, navigating

database concepts, e.g.:
components of database systems;
design of core DBMS functions (e.g. query mechanisms, access methods);
database architecture and query language

big data, e.g.: benefits and limitations, components and architectures employed in systems for big data (e.g. Hadoop cluster, JSON) ,
tools and techniques for analysing large heterogeneous data sets, including statistics

graph theory

key concepts and benefits of information security management system

internationally recognised standards – e.g., ISO27001, or similar

governance, organisational structure, roles, policies, standards and guidelines for cyber and information security

how an organisation's security policies, standards and governance are supported by provisioning and access rights – e.g., how identity and access management are implemented and maintained for a database application or physical access control system

how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations

the roles of experts in the cyber security industry, how they are recognised, and the work they do.

how to use organisations such as a CERT, OSINT provider, incident response provider

Teaching and Learning Methods: The initial part of the module teaches students the basic concepts of information management and how to use database management systems.

The latter part covers the standards, policies and procedures for information security. These will cover human behaviour as well as physical and electronic assets.

Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.

Part 3: Assessment

Part 3: Assessment

This module is assessed by a combination of techniques: a presentation and two reports.
Component A:
A presentation (30 minutes) of an information security plan for the apprentice's organisation. It should cover:
Compliance with ISO27001
The organisation's security policies and procedures
The use of CERT and OSINT

This allows the students to contextualise their theoretical knowledge within the context of an organisation with which they are familiar and brings to life the challenges of auditing and managing information assets.

Component B of assessment allows the students to concentrate on an alternative aspect of security management, the management of data. In the first part of this assessment students will design, create and use a database through a DBMS and explain information concepts (1,500 words or equivalent) . Having demonstrated their grasp of the technicalities of data management, in the second part of the assessment they will deal with the presentation and operational aspects of data management by extracting and presenting data (including graphs) from a large dataset. They will explain potential issues with the management of large datasets (1,500 words)

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A		50 %	20 minute presentation and 10 minute Q&A session.
Report - Component B		25 %	Report (1,500 words)
Report - Component B	✓	25 %	Report on the management of a large dataset (1,500 words).
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A		50 %	Presentation (20 mins presentation and 10 mins Q&A)
Report - Component B		25 %	Report (1,500 words)
Report - Component B		25 %	Report (1,500 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**
Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment.	MO1
Select an appropriate management system and use it to develop an information security management plan.	MO2
Explain the key concepts of information management.	MO3
Design a relational database using best practice techniques	MO4
Create and use a database via a DBMS .	MO5

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	135
Total Independent Study Hours:	135
Placement Study Hours:	
Placement	75

	Total Placement Study Hours:	75
	Scheduled Learning and Teaching Hours:	
	Face-to-face learning	90
	Total Scheduled Learning and Teaching Hours:	90
	Hours to be allocated	300
	Allocated Hours	300
Reading List	*The reading list for this module can be accessed via the following link:* https://rl.talis.com/3/uwe/lists/CD43F295-21E6-83F5-3D12-BB3533A50A76.html	

Part 5: Contributes Towards
This module contributes towards the following programmes of study: Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [Sep][FT][GlosColl][3yrs] BSc (Hons) 2020-21