STUDENT AND ACADEMIC SERVICES

MODULE SPECIFICATION

Part 1: Information			
Module Title	Computer Network Security [TSI]		
Module Code	UFCFPX-6-3	Level	Level 6
For implementation from	2023-24		
UWE Credit Rating	6	ECTS Credit Rating	3
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		
PSRB Requirements	None		

Part 2: Description

Educational Aims: Provide an in-depth, theoretical understanding of network security. Provide students with the knowledge and skills necessary to design and support network security.

Outline Syllabus: •   Modern Network Security Threats
•   Securing Network Devices
•   Authentication, Authorization and Accounting
•   Implementing Firewall Technologies
•   Implementing Intrusion Prevention
•   Securing the Local Area Network
•   Cryptography
•   Managing a Secure Network

Teaching and Learning Methods: Learning and teaching will be provided to students in two forms: lectures and labs. During lectures, theoretical aspects of the course will be provided to students by the teaching staff. Lectures will be supported by presentation published and available to the students on e.tsi.lv under the module section. Also, additional materials, like text books,

publications on the internet, videos etc will be presented in e.tsi.lv. During labs, each student receives an individual task to perform

Part 3: Assessment
This module assessment is split into two components (A – Exam, B – Practical Assignments): A1 - final 1-hour examination which will assess the students understanding of taught material that forms part of the learning outcomes but cannot easily be assessed through practical tasks. B1 – A portfolio of labs, test topics covered in this module. For each lab students should produce a report.

First Sit Components	Final Assessment	Element weighting	Description
Portfolio - Component B		40 %	A portfolio of labs, test topics covered in this module. For each lab students should produce a report.
Examination - Component A		60 %	MQC Examination
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Portfolio - Component B		40 %	A portfolio of labs, test topics covered in this module. For each lab students should produce a report.
Examination - Component A		60 %	MCQ Examination

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
Describe the security threats facing modern network infrastructures and identify some of the factors driving the need for network security	MO1
Identify and classify particular examples of attacks	MO2
Identify physical points of vulnerability in simple networks	MO3
Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack and explain the characteristics of hybrid systems	MO4
Secure network device access and implement AAA on network devices	MO5
Mitigate threats to networks using ACLs	MO6
Implement secure network management and reporting	MO7
Mitigate common Layer 2 attacks	MO8
Administer effective security policies	MO9

Contact Hours	**Independent Study Hours:**	
	Independent study/self-guided study	48

	Total Independent Study Hours:	48
		3
	Scheduled Learning and Teaching Hours:	
	Face-to-face learning	32
	Total Scheduled Learning and Teaching Hours:	32
	Hours to be allocated	60
	Allocated Hours	80
Reading List	*The reading list for this module can be accessed via the following link:* https://rl.talis.com/3/uwe/lists/B48CD3D8-239B-60C5-EEDA-850F4137EB15.html?lang=en-gb&login=1	

Part 5: Contributes Towards
This module contributes towards the following programmes of study: Computer Science and Software Development [Oct][FT][TSI][4yrs] BSc (Hons) 2020-21 Computer Science and Software Development [Feb][FT][TSI][4yrs] BSc (Hons) 2020-21