University of the West of Scotland

Module Descriptor

Session: 2024/25

Title of Module: Security Fundamentals			
Code: COMP07075	**SCQF Level: 7 (Scottish Credit and Qualifications Framework)**	**Credit Points: 20**	**ECTS: 10 (European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Raman Singh		

Summary of Module

This module aims to provide students with fundamentals of security, including general security architecture and principles of secure design, cryptography, and system threats & vulnerabilities. This module also introduces security issues of data, network and software development that affect the ICT systems.

In addition, general ethical and legal issues and general organisational operations of secure systems are also provided to give students an overview of operating secure systems. Undertaking this module will develop a range of graduate attributes. Knowledge and understanding of the principles and techniques used to secure the data and information for current and future applications.

This module will work to develop a number of the key 'I am UWS' Graduate Attributes to make those who complete this module:

- Universal: Critical Thinker, Ethically minded, Research-minded
- Work Ready: Problem-Solver, Effective Communicator, Ambitious
- Successful: Autonomous, Resilient, Driven

Module Delivery Method

Face-To-Face	**Blended**	**Fully Online**	**HybridC**	**Hybrid 0**	**Work-Based Learning**
☒	☒	☐	☐	☐	☐

See Guidance Note for details.

Campus(es) for Module Delivery						
The module will **normally** be offered on the following campuses / or by Distance/Online Learning: (Provided viable student numbers permit) (tick as appropriate)						
Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
☐	☐	☐	☒	☐	☐	Add name

Term(s) for Module Delivery					
(Provided viable student numbers permit).					
Term 1	☐	Term 2	☒	Term 3	☐

Learning Outcomes: (maximum of 5 statements) **These should take cognisance of the SCQF level descriptors and be at the appropriate level for the module.** At the end of this module, the student will be able to:	
L1	Demonstrate a critical understanding of the general architecture of the secure systems and designing principles of security, including legal and ethical issues;
L2	Demonstrate detailed knowledge of operating systems as well as knowledge of networking fundamentals including the OSI model;
L3	Demonstrate a deep understanding of the weaknesses & vulnerability of systems and access control to these systems;
L4	Demonstrate a good understanding of cryptography and its applications;
L5	Effectively apply security measures to protect data, networks, and software;

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	During completion of this module, there will be an opportunity to achieve core skills in:
Knowledge and Understanding (K and U)	SCQF Level **7** A detailed understanding of computers, networks, operating systems, security architecture and design principles, cryptography applications, access control, and legal and ethical issues.
Practice: Applied Knowledge and Understanding	SCQF Level **7** The ability to effectively apply security measures to protect data, networks, and software.

Generic Cognitive skills	SCQF Level **7** Skills in identifying and analysing security threats.	
Communication, ICT and Numeracy Skills	SCQF Level **7** Skills in designing secure systems, report writing and presentation skills.	
Autonomy, Accountability and Working with others	SCQF Level **7** Ability to work in a team.	
Pre-requisites:	Before undertaking this module, the student should have undertaken the following:	
	Module Code:	**Module Title:**
	Other:	
Co-requisites	**Module Code:**	**Module Title:**

*Indicates that module descriptor is not published.

Learning and Teaching	
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.	
Learning Activities During the completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Normally totalling 200 hours): (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	12
Tutorial/Synchronous Support Activity	12
Laboratory/Practical Demonstration/Workshop	24
Independent Study	152
	200 Hours Total
****Indicative Resources: (eg. Core text, journals, internet access)**	

The following materials form the essential underpinning for the module content and ultimately for the learning outcomes: Eastom, C. (2023) Computer Security Fundamentals (5th Edition). Pearson. Panek, C. (2019) Security Fundamentals (1st Edition). Sybex Stallings, W and Brown, L. (2017) Computer Security: Principles and Practice. (4th Edition). Pearson.
(**N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)
Attendance and Engagement Requirements
In line with the Student Attendance and Engagement Procedure: Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time.

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Please ensure any specific requirements are detailed in this section. Module Co-ordinators should consider the accessibility of their module for groups with protected characteristics..
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	Computing
Assessment Results (Pass/Fail)	Yes ☐No ☒
School Assessment Board	Business & Applied Computing
Moderator	Sean Sturley

External Examiner	M Davis
Accreditation Details	e.g. ACCA Click or tap here to enter text.
Changes/Version Number	1.08

Assessment: (also refer to Assessment Outcomes Grids below)
Assessment 1 – Practical Coursework (60%)
Assessment 2 – Group Project (40%)
(N.B. (i) **Assessment Outcomes Grids** for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An **indicative schedule** listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Assessment Outcome Grids (See Guidance Note)

Component 1							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Report of practical/field/ clinical work	✓	✓	✓	✓		60	0

Component 2							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Dissertation/ Project report/Thesis					✓	40	0
Combined Total for All Components						**100%**	**0 hours**

Change Control:

What	When	Who
Further guidance on aggregate regulation and application when completing template	16/01/2020	H McLean
Updated contact hours	14/09/21	H McLean
Updated Student Attendance and Engagement Procedure	19/10/2023	C Winter
Updated UWS Equality, Diversity and Human Rights Code	19/10/2023	C Winter
Guidance Note 23-24 provided	12/12/23	D Taylor
General housekeeping to text across sections. .	12/12/23	D Taylor

Version Number: MD Template 1 (2023-24)