University of the West of Scotland

Module Descriptor

Session: 2024/25

Title of Module: Foundations of Cyber Security			
Code: COMP11080	**SCQF Level: 11 (Scottish Credit and Qualifications Framework)**	**Credit Points: 10**	**ECTS: 5 (European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Raman Singh		

Summary of Module

This module provides a complete overview of all the essential aspects of Cyber Security ranging from basic terminologies to securing a cyber-physical system. The module covers a discreet introduction to cyber security concepts, ethical hacking, web security, security operations and cyber-physical system security. This module also discusses various vectors of security attacks and threats. This module further discusses various policies, standards and procedures governed nationally and internationally. This module also covers a group-based assignment to acquire relevant and up-to-date trends, challenges, and scope in the domain of information and cyber security.

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 basic concepts, terminology and technologies of cyber security;
L2	Demonstrate a critical understanding of cyber threats and the corresponding detection and defence techniques;
L3	Learn the basic principles of SecOps, including the security risks & challenges;
L4	Demonstrates how to incorporate best-practice security into the development and deployment of workflows.

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 **11** Students will learn about basic concepts, terminology and technologies of cyber security.
Practice: Applied Knowledge and Understanding	SCQF Level **11** Students will gain an in-depth, comprehensive understanding and critical awareness of knowledge of cyber security and use techniques to secure business operations and workflows.
Generic Cognitive skills	SCQF Level **11** To complete their written reports and laboratory tasks, students will first build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry.

Communication, ICT and Numeracy Skills	SCQF Level **11** Working in groups, students will develop communication skills as well as the ability to write technical reports and documentation.	
Autonomy, Accountability and Working with others	SCQF Level **11** Exercise a substantial ability to work autonomously, demonstrating critical inquiry in producing quality work underpinned by rigorous investigation. Learn effectively for the purpose of continuing personal development planning through interacting with others in academic and fellow students.	
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 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	6
Tutorial/Synchronous Support Activity	6
Laboratory/Practical Demonstration/Workshop	12
Independent Study	76
	100 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. Graham, D. (2021) Ethical Hacking: A Hands-On Introduction to Breaking. No Starch Press. Chapple M., Stewart J.M., Gibson D., Seidl D. (2021) (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide & Practice Tests Bundle. (3rd Edition). Sybex.
(**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	Steve Eager

External Examiner	N Coull
Accreditation Details	e.g. ACCA Click or tap here to enter text.
Changes/Version Number	1.07

Assessment: (also refer to Assessment Outcomes Grids below)
Practical Coursework (60%)
Group Research Report (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)**	**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)**	**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)