University of the West of Scotland

Undergraduate Programme Specification

Session: 2022/23

Last modified: 07/07/2022 14:52:04

Named Award Title:	**MEng (Hons) Cyber Security Single**

Award Title for Each Award:	**MEng (Hons) Cyber Security** **BEng (Hons) Cyber Security** **BEng Cyber Security** **Dip HE Computing** **Cert HE Computing**

Awarding Institution/Body:	University of the West of Scotland
Language of Instruction & Examination:	English
Award Accredited By:	Seeking Accreditation from BCS, IISP, NCSC
Maximum Period of Registration:	7 Yrs - Full Time, 10 Yrs - Part Time
Mode of Study:	Full Time Part Time
Campus:	Lanarkshire

School:	School of Computing, Engineering and Physical Sciences
Programme Leader:	Sean Sturley

Admission Criteria

Candidates must be able to satisfy the general admission requirements of the University of the West of Scotland as specified in Chapter 2 of the University Regulatory Framework together with the following programme requirements:

SQA National Qualifications

Grades A, B, B, B @ Higher including Mathematics or Physics.

---

or GCE

Grades B, B, B @ A level, including Mathematics or Physics.

---

or SQA National Qualifications/Edexcel Foundation

An appropriate HNC/HND award with an 'A' in the Graded Unit.

Year 2 entry with an HNC with an 'A' in the Graded Unit.

Year 3 entry with an HND with an 'A' in the Graded Unit.

The level of entry and/or credit awarded being subject to the content of the HN programme.

Other Required Qualifications/Experience

Applicants may also be considered with other academic, vocational or professional qualifications deemed to be equivalent.

Further desirable skills pre-application

General Overview

This programme has been devised to meet a growing need, as identified by the Scottish and UK Governments, for individuals who possess a skillset to meet the challenges posed by the constantly evolving computer systems that they may be employed to support today.

There is currently a short supply of highly skilled cyber professionals. Therefore this programme will produce graduates with the skillset to fill this gap by teaching them in such a way that they can identify, assess and evaluate cyber security threats and attacks, and in turn work with others to develop robust and secure solutions using best practice frameworks.

This exciting programme has been developed with due cognisance of the IISP and NCSC (National Cyber Security Centre) frameworks. The integration of academia and industry in delivering the programme will ensure the currency of this innovative industry focussed programme.

Graduate Attributes, Employability & Personal Development Planning

Graduate Attributes

UWS Graduate Attributes focus on academic, personal and professional skills and throughout the programmes that these skills develop graduates who are universally prepared, work-ready and successful. The Cyber Security programme provides opportunities throughout the levels to enable these skills to be developed and focussed appropriately.

Critical analytical and inquiry skills are developed and used to solve industry related problems wherever possible. The programme promotes cultural awareness and emotional intelligence with a variety of group exercises developing resilient, ambitious and enterprising leadership qualities whilst ensuring that group members are emotionally and culturally aware and respectful communication and behaviours are the norm.

Ethical awareness and social responsibility is developed throughout and is formalised in 4th year during project studies where School/University ethical approval is sought if required.

Links to current University and programme research are promoted through the programme with opportunities for students to become involved in aspects of the research from the earliest opportunity either discretely or as part of an assessment.

Employability – The School regularly receives interest from companies to engage with our students and we are keen to facilitate this where we see benefits for our students. The School also runs a number of specific employability events at the Lanarkshire and/or Paisley campuses, including an employer speed networking events and an annual ‘Working with Industry’ event. Invited Industrial speakers and former students will also provide input to the programme.

Personal Development Planning (PDP) within the programme is based on four strands: personal tutor support, a number of modules linked to PDP outcomes, support for development of an ePortfolio, and a number of events relating to PDP.

A personal tutor is identified for each student, and students are expected to meet with their personal tutors on a regular basis - at least once per term - to discuss issues relating to PDP, including progress, development goals and aspirations.

A number of modules core to the programme at each level have been identified as being strongly linked to PDP themes, and these are:

First year: COMP07067 Professional Development in Computing

Second year: embedded in several of the modules.

Third year: COMP09093 Professional Computing Practice

Honours year: COMP10034 Computing Honours Project and COMP10074 Advanced Professional Practice in Computing

Employability – The School regularly receives interest from companies to engage with our students and we are keen to facilitate this where we see benefits for our students. The School also runs a number of specific employability events at the Lanarkshire and/or Paisley campuses, including an employer speed networking events and an annual ‘Working with Industry’ event. Invited Industrial speakers and former students will also provide input to the programme.

Personal Development Planning (PDP) within the programme is based on four strands: personal tutor support, a number of modules linked to PDP outcomes, support for development of an ePortfolio, and a number of events relating to PDP.

A personal tutor is identified for each student, and students are expected to meet with their personal tutors on a regular basis - at least once per term - to discuss issues relating to PDP, including progress, development goals and aspirations.

A number of modules core to the programme at each level have been identified as being strongly linked to PDP themes, and there are also specific PDP modules in 1st, 3rd and 4th year of the programme.

First year: COMP07067 Professional Development in Computing

Second year: embedded in several of the modules.

Third year: COMP09093 Professional Computing Practice

Honours year: COMP10034 Computing Honours Project and COMP10074 Advanced Professional Practice in Computing

Fifth year: COMP11083 Individual Research Project

UWS provides support for development of an online ePortfolio through the Mahara system.

Finally, a number of events relating to PDP take place throughout the year, which may be associated with the School, campus or programme.

Work Based Learning/Placement Details

Students will be encouraged to actively engage in summer internships and placements throughout the programme of study, and have the option to complete an industrial (sandwich) placement year, to ensure the relevance of skills development as applied to industry is established. To facilitate these activities, students will be given opportunities to network with professional practitioners through supported activities and given workshops on developing techniques of networking.

Engagement

In line with the Academic Engagement Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on the relevant learning platform, 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 and Diversity Policy

Programme structures and requirements, SCQF level, term, module name and code, credits and awards (Chapter 1, Regulatory Framework)

A. Learning Outcomes (Maximum of 5 per heading)

Outcomes should incorporate those applicable in the relevant QAA Benchmark statements

Knowledge and Understanding	
A1	Describe and explain the dynamic nature of the cyber security sector.
A2	Define and discuss the key areas, concepts and principles of cyber security.
A3	Describe and explain the standard mathematical and statistical concepts used in computing.
Practice - Applied Knowledge and Understanding	

B1	Develop computing applications by applying knowledge and understanding of the principles and techniques of structured programming.
B2	Compile, execute, debug and document software using a current Integrated Development Environment (IDE).
B3	Employ the professional skills, techniques, practices and/or materials associated with cyber security.
Communication, ICT and Numeracy Skills	
C1	Solve problems of a non-routine nature in creative and innovative ways.
C2	Practise numeracy in understanding and presenting cases involving a quantitative dimension.
C3	Use a range of ICT applications to support and enhance work and adjust features to suit purpose.
C4	Practise communication skills in electronic as well as written and oral form to a range of audiences.
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Coherently present and evaluate arguments, information and ideas.
D2	Participate within the legal, ethical and professional framework within which they study.
Autonomy, Accountability and Working With Others	
E1	Define and explain key issues in relation to the accountability and responsibilities of computer professionals to clients, the community, and society at large.
E2	Manage limited resources within defined areas of computing work.

Core Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
7	COMP07009	Introduction to Web Development	20	✓			
7	COMP07012	CCNA1: Introduction to Networks	20		✓		
7	COMP07027	Introduction to Programming	20	✓	✓		
7	COMP07061	Computing Systems	20	✓			
7	COMP07067	Professional Development in Computing	10	✓			
7	COMP07075	Security Fundamentals	20		✓		
7	MATH07005	Mathematics for Computing	10		✓		

* Indicates that module descriptor is not published.

Footnotes

Optional Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	

* Indicates that module descriptor is not published.

Footnotes

Criteria for Progression and Award

To progress from SCQF Level 7 to SCQF Level 8 in this programme, students are normally required to obtain 120 credits from the above programme and achieve an average of all modules of >=60%.

All pre-requisite modules must be passed before progression is allowed.

Refer to Regulation 3.13 regarding progression with credit deficit, note, the decision to permit a proceed with carry is

not automatic but is subject to detailed discussion at the programme award board.

Students obtaining 120 credits at SCQF Level 7 or above, with 100 from the programme are eligible for the exit award of the Certificate of Higher Education in Computing.

B. Learning Outcomes (Maximum of 5 per heading)

Outcomes should incorporate those applicable in the relevant QAA Benchmark statements

Knowledge and Understanding	
A1	Define and explain the concepts and principles of the object-oriented paradigm in the development of computing applications.
A2	Identify and explain the importance of data abstraction and the role this plays in computing.
A3	Demonstrate an intellectual understanding of, and an appreciation for, the central role of algorithms and data structures, and work with a variety of them.
A4	Identify and explain the key aspects of relational database theory.
Practice - Applied Knowledge and Understanding	
B1	Analyse the extent to which a proposed or existing computer-based application meets the criteria defined for its intended use.
B2	Use a range of routine and advanced skills, techniques and practices to develop software.
B3	Analyse a new or existing workplace system and design and implement a relational database to better meet company the requirements.
Communication, ICT and Numeracy Skills	
C1	Present a reasoned and evidence-based proposal for a computer-based solution to meet an identified need in the work place.
C2	Employ routine and specialised software development skills. For example, use a range of standard applications to process and obtain data.
C3	Utilise a database to store and retrieve information effectively.
C4	Employ routine and specialised network penetration testing and ethical hacking skills.
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Employ a range of approaches to formulate evidence-based solutions/ responses to defined and/or routine cyber security problems/issues.
D2	Critically evaluate and analyse evidence-based solutions/responses to defined and/or routine cyber security problems/ issues.
Autonomy, Accountability and Working With Others	
E1	Deal with ethical and professional issues in accordance with current professional and/or ethical codes or practices in the discipline of computing science as a whole and cyber security specifically, under guidance.
E2	Identify and apply current professional and/or ethical codes or practices in the discipline of computing science as a whole and cyber security, specifically.

Core Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
8	COMP08002	Database Development	20	✓			
8	COMP08074	Operating Systems	20	✓			
8	COMP08094	Ethical Hacking: Tools & Techniques	20		✓		

8	COMP08100	Linux: Tools and Administration	20	✓			

* Indicates that module descriptor is not published.

Footnotes
1. COMP07027 - Introduction to Programming, is offered, as an alternative to COMP08101 - Programming for Cyber Security, for direct entry students to Yr 2 with no previous programming experience.

2. MATH07005 - Mathematics for Computing, is core for direct entry students. This will result in additional credit for direct entrants.

Optional Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
7	MATH07005	Mathematics for Computing	10		✓		See Note 1.
7	COMP07027	Introduction to Programming	20	✓	✓		See Note 2.
		Or					
8	COMP08101	Programming for Cyber Security	20	✓			See Note 2.
8	COMP08097	CCNA2 Switching Routing & Wireless Essentials	20		✓		See Note 3.
		Or					
9	COMP09115	CCNA1/2: Networks, Routing, Switching & WLANs	30	✓	✓		See Note 3.

* Indicates that module descriptor is not published.

Footnotes
1. MATH07005 - Mathematics for Computing, is core for direct entry students. This will result in additional credit for direct entrants.

2. COMP07027 - Introduction to Programming, is offered, as an alternative to COMP08101 - Programming for Cyber Security, for direct entry students to Yr 2 with no previous programming experience.

3. COMP09115 - CCNA1/2: Networks, Routing, Switching & WLANs, is offered, as an alternative to COMP08097 - CCNA2 Switching Routing & Wireless Essentials, for direct entry students to Yr 2 with no previous programming experience. This will result in additional credit for direct entrants.

Criteria for Progression and Award

To progress from SCQF Level 8 to SCQF Level 9 in this programme, students are required to obtain 240 credits from the above programme and achieve an average of all modules in the year of >=60%.

All pre-requisite modules must be passed before progression is allowed.

Refer to Regulation 3.13 regarding progression with credit deficit, note, the decision to permit a proceed with carry is not automatic but is subject to detailed discussion at the programme award board.

Students obtaining 240 credits of which 100 are at SCQF Level 8 or above from the programme are eligible for the exit award of the Diploma of Higher Education in Computing.

C. Learning Outcomes (Maximum of 5 per heading)

Outcomes should incorporate those applicable in the relevant QAA Benchmark statements

Knowledge and Understanding	
A1	Demonstrate a critical understanding of relevant cyber security principles and practice.
A2	Demonstrate a critical understanding of the scope, main areas and boundaries of cyber security.
A3	Analyse theories, principles, concepts and terminology associated with cyber security.

Practice - Applied Knowledge and Understanding	
B1	Practise routine methods of enquiry and research associated with computing science.
B2	Apply the principal skills, techniques, practices and/or materials associated with cyber security.
B3	Practise routine methods of enquiry and/or research associated with cyber security.
Communication, ICT and Numeracy Skills	
C1	Use a range of tools and techniques associated with cyber security.
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Understand and apply a range of computing concepts, principles and practices in the context of well specified scenarios, exercising judgement in the selection of tools and techniques.
D2	Draw on a range of sources in making judgements.
Autonomy, Accountability and Working With Others	
E1	Recognise and deal with the professional, economic, social, environmental, moral and ethical issues involved in the sustainable exploitation of computer technology, and be guided by the adoption of appropriate professional, ethical and legal practices in the work place.
E2	Use initiative in managing ethical and professional issues in accordance with current professional and/or ethical codes or practices.

Core Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
9	COMP09092	Research Methods in Computing	10		✓		
9	COMP09093	Professional Computing Practice	10	✓			
9	COMP09106	Cryptography	20	✓			
9	COMP09107	Digital Forensic Analysis	20	✓			
9	COMP09111	Systems Programming Concepts	20		✓		

* Indicates that module descriptor is not published.

Footnotes

Optional Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
7	MATH07005	Mathematics for Computing	10		✓		See Note 1.
9	COMP09110	Python for Network Engineers	10		✓		See Note 2.
		And					
8	COMP08101	Programming for Cyber Security	20	✓			
9	COMP09115	CCNA1/2: Networks, Routing, Switching & WLANs	30	✓	✓		See Note 3.
		Optional Modules can be chosen from the following:					
9	COMP09024	Unix System Administration	20	✓			
9	COMP09086	Information Security Management	20		✓		

9	COMP09109	Web Application Security Testing	20		✓		
9	COMP09116	CCNA: CyberOps	20	✓			

* Indicates that module descriptor is not published.

Footnotes
1. MATH07005 - Mathematics for Computing, is offered as an additional module for direct-entry students to Yr 3 as an additional module for those students wishing to refresh their Maths knowledge. This will result in additional credit for direct-entry students.

2. COMP08101 - Programming for Cyber Security and COMP09110 - Python for Network Engineers, are offered as preferred additional modules for direct entry students to Yr 3 with no previous programming experience. This may result in additional credit for direct-entry students.

3. COMP09115 - CCNA1/2: Networks, Routing, Switching & WLANs is core for direct entry students to Yr 3 with no previous networking experience. This will result in additional credit for direct-entry students.

Criteria for Progression and Award

To progress from SCQF 9 to SCQF 10 in this programme, students are required to obtain 360 credits of which 100 credits are at SCQF 9 from the above programme and to achieve an average in all modules of at least 60% in every year of study, inclusive of SCQF Level 9. Students who do not achieve at least 60% may be eligible to transfer to the BEng programme.

All pre-requisite modules must be passed before progression is allowed and no student will be allowed to progress to Level 10 with credit deficit.

Students obtaining 360 credits of which 100 are at SCQF 9 or above from the programme are eligible for the exit award of the BEng Cyber Security.

The award of distinction can be made to a student obtaining a pass degree as stated in the University Regulations.

D. Learning Outcomes (Maximum of 5 per heading)

Outcomes should incorporate those applicable in the relevant QAA Benchmark statements

Knowledge and Understanding	
A1	Demonstrate and work with a knowledge that covers and integrates most of the principal areas, features, boundaries, terminology and conventions within cyber security.
A2	Demonstrate a critical understanding of the principal theories, concepts and principles conventions within the selected area of cyber security study, some of which are informed by or at the forefront of the selected theme(s) of study.
A3	Demonstrate knowledge and understanding of cyber security including a range of established techniques of enquiry or research methodologies.
Practice - Applied Knowledge and Understanding	
B1	Execute a defined project of research, development or investigation within the area of cyber security and identify and implement relevant outcomes.
B2	Critically review and assess contributions to the research literature of cyber security.
B3	Use a range of the principal skills, practices and/or materials associated within the selected theme(s) of study in a project.
B4	Use and integrate skills, practices and/or materials which are specialised, advanced, or at the forefront of cyber security.
Communication, ICT and Numeracy Skills	
C1	Deliver a coherent and reflective presentation of an extended piece of project work to an informed audience.
C2	Produce a critical and evaluative written report of a development project.
C3	Use a wide range of routine and specialised skills in support of established practices within the selected theme(s) of study - for example: - make formal presentations about specialised topics to informed audiences

	- use a range of software to support and enhance work at this level and specify refinements/ improvements to software to increase effectiveness, - interpret, use and evaluate a range of numerical and graphical data to set and achieve goals/ targets.
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Critically analyse and apply a range of computing concepts, principles and practices in the context of loosely defined problems where information is limited and/or comes from a range of sources, exercising judgement in the selection of tools and techniques.
D2	Critically review and consolidate knowledge, skills and practices and thinking within the selected theme(s) of study.
D3	Demonstrate originality and creativity in dealing with professional level computing issues.
Autonomy, Accountability and Working With Others	
E1	Practise in ways which show a clear awareness of own and others' roles and responsibilities.
E2	Deal with complex ethical and professional issues in accordance with current professional and/or ethical codes or practices.

Core Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
10	COMP10068	Secure Programming	20		✓		
10	COMP10073	Advanced Digital Forensic Analysis	20	✓			
10	COMP10075	Governance, Risk & Compliance	20		✓		
10	COMP10076	Group Research Project	40	✓	✓		

* Indicates that module descriptor is not published.

Footnotes

Optional Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
		For T1 students can select from:					
10	COMP10014	Network Security	20	✓			
		Or					
10	COMP10082	Machine Learning for Data Analytics	20	✓			

* Indicates that module descriptor is not published.

Footnotes

Criteria for Progression and Award

To progress from SCQF 10 to SCQF 11 in this programme, students are normally required to obtain 480 credits from the above programme and achieve an average of 60% in all modules at SCQF Level 9 & 10.

Students obtaining 480 credits of which 240 are at SCQF 9 and SCQF 10 from the above programme including all core modules but do not satisfy the requirements for progression to Level 11 are eligible for the BEng (Hons) Cyber Security Award.

E. Learning Outcomes (Maximum of 5 per heading)

Outcomes should incorporate those applicable in the relevant QAA Benchmark statements

Knowledge and Understanding

A1	Demonstrate an advanced knowledge and a critical and comprehensive understanding of the principal theories, concepts and principles related to computer science which underpin cyber security and an awareness of the contemporary issues at the forefront of professional practise.
A2	Demonstrate an advanced knowledge and a critical and comprehensive understanding of the essential principles and practices of the domain including current standards, processes, principles and the most appropriate software; the reasons for their relevance to professional practice.
Practice - Applied Knowledge and Understanding	
B1	Demonstrate the ability to critically analyse, extend and apply knowledge, skills, practices and thinking.
B2	Apply critical analysis, evaluation and synthesis to forefront issues, or issues informed by forefront developments in cyber security and the underpinning computer science discipline.
B3	Identify, conceptualise, analyse and define new and abstract problems given practical constraints.
Communication, ICT and Numeracy Skills	
C1	Use a range of ICT applications to support and enhance work and adjust features to suit purpose.
C2	Use communication skills in electronic as well as written and oral form to a range of audiences.
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Develop original, creative and innovative responses to professional challenges, problems and issues.
D2	Deal with complex issues and make informed judgements in situations in the absence of data.
Autonomy, Accountability and Working With Others	
E1	Participate within the legal, ethical and professional framework within which they study.
E2	Plan self-learning and improve performance as a foundation for on-going professional development.
E3	Exercise substantial autonomy and initiative in professional and equivalent activities.

Core Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
11	COMP11024	Masters Project	60		✓		
11	COMP11093	Mobile Forensics	20	✓			
11	COMP11090	Malware Analysis & Reverse Engineering	20	✓			

* Indicates that module descriptor is not published.

Footnotes

Optional Modules

SCQF Level	Module Code	Module Name	Credit	Term			Footnotes
				1	2	3	
		20 credits are to be chosen from the following optional modules:					
11	COMP11076	Advanced Network Security	10		✓		
11	COMP11077	Applied Cryptography	10		✓		
11	COMP11082	Incident Response	10		✓		
11	COMP11086	Cyber Security: Law and Ethics	10	✓			
11	COMP11094	Network Penetration Testing	10	✓			

11	COMP11099	Threat Intelligence	10		✓		

* Indicates that module descriptor is not published.

Footnotes

Criteria for Award

To be eligible for the award of MEng (Hons) degree a candidate must hold 600 credits, including 360 at SCQF Levels 9, 10 and 11 from the above programme.

The Classification will take into account students' performance at Level 9, Level 10 and Level 11.

The composite mark is given by:
20% from Level 9
30% from Level 10
50% from Level 11

The classification will be determined as follows:-
First Class >=70% Average
Upper Second Class (2.1) >=60% Average
Lower Second Class (2.2) >=50% Average

Regulations of Assessment

Candidates will be bound by the general assessment regulations of the University as specified in the University Regulatory Framework.

An overview of the assessment details is provided in the Student Handbook and the assessment criteria for each module is provided in the module descriptor which forms part of the module pack issued to students. For further details on assessment please refer to Chapter 3 of the Regulatory Framework.

To qualify for an award of the University, students must complete all the programme requirements and must meet the credit minima detailed in Chapter 1 of the Regulatory Framework.

Combined Studies

There may be instances where a student has been unsuccessful in meeting the award criteria for the named award and for other more generic named awards existing within the School. Provided that they have met the credit requirements in line with the SCQF credit minima (please see Regulation 1.21), they will be eligible for an exit award of CertHE / DipHE or BA / BSc in Combined Studies.

For students studying BA, BAcc, or BD awards the award will be BA Combined Studies.

For students studying BEng or BSc awards, the award will be BSc Combined Studies.

Version Number: 1.05