Integrated Masters Programme Specification

Session	2025/26	**Last Modified**	
Named Award Title	MEng (Hons) Cyber Security		
Award Title for Each Award	MEng (Hons) Cyber Security BEng (Hons) Cyber Security BEng Cyber Security Dip HE Cyber Security Cert HE Computing		
Date of Approval	30/05/2025		
Details of Cohort Applies to	2025/26		
Awarding Institution	University of the West of Scotland	**Teaching Institution(s)**	University of the West of Scotland
Language of Instruction & Examination		English	
Award Accredited by			
Maximum Period of Registration		Full Time – 7 years; Part Time – 10 years;	
Duration of Study			
Full-time	5 Years	**Part-time**	8 Years
Placement (compulsory)	No		
Mode of Study	☒ Full-time ☒ Part-time		
Campus	☐ Ayr ☐ Dumfries	☒ Lanarkshire ☐ London ☐ Paisley	☐ Online / Distance Learning ☐ Other (specify)
School	**Computing, Engineering and Physical Sciences**		
Divisional Programme Board	**Computing**Error! Bookmark not defined.		
Programme Leader	Raman Singh		

Admissions 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:

Scottish Highers

· Standard Entry Requirements: ABBB (114 UCAS Tarrif points) including Maths/Applications of Maths and Physics, plus National 5 English (or equivalent) at B or above

Or GCE

A Levels: BBC (112 UCAS Tarrif points) including Maths and Physics plus GCSE English

Or SQA National Qualifications / Edexcel Foundation

Other Required Qualifications/Experience

Irish Leaving Certificate: H2H2H2H3 including Maths and Physics, plus English at Ordinary Level

International Baccalaureate: 32 points including Maths and Physics, plus English at Standard Level.

BEng (Hons)

Scottish Highers

· Standard Entry Requirements: BBBC (102 UCAS Tarrif points) including Maths, Computing or Physics

· Minimum Entry Requirements: BBCC (96 UCAS Tarrif points) including Maths, Computing or Physics

A Levels: CCC (96 UCAS Tarrif Points) including Maths, Computing or Physics

Irish Leaving Certificate: H3H3H3H4 including Maths, Computing or Physics

International Baccalaureate: 24 points including Maths, Computing or Physics

Scottish Wider Access Programme: Access to STEM (BBB)

Year 2 ENTRY (BEng Only)

Scottish Advanced Highers: CCD (112 UCAS Tarrif points) including Computing or evidence of programming

A Levels: BBC (112 UCAS Tarrif points) including Computing or evidence of programming

International Baccalaureate: 28 points including Computing or evidence of programming

BTEC Extended Diploma: DDM

SQA HNC/BTEC Level 4 HNC: Networking (with programming); Cyber Security; Computing Science (with networking modules)

Year 3 Entry (BEng Only)

Further desirable skills pre-application

SQA HND/BTEC Level 5 HND: Networking (with programming); Cyber Security; Computing Science (with networking modules); Information Security.

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.
The exciting programme has been developed with due cognisance of the IISP (Chartered Institute of Cyber Security) 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-focused programme.
The MEng (Hons) Cyber Security course provides an in-depth education in central subjects like Networking, Digital Forensics, and Ethical Hacking, providing learners with critical technical know-how. As the course proceeds, it covers sophisticated subjects like IoT Security, Advanced Network Security, and Cyber Laws, getting the graduates ready for the changing world of cyber attacks. Through a combination of practical experience and theoretical knowledge, the course is framed to create highly competent professionals capable of handling intricate cybersecurity issues.

Typical Delivery Method

Students are expected to attend classes in Face-to-Face mode. Most modules have mandatory lab work. Most modules have either 20 credits or 10 credits of weightage. The module study material is delivered over 12 weeks for the 20-credit module and 6 weeks for the 10-credit module. Each module is expected to engage on a weekly basis, mostly in 4-hour sessions. Each term, students are offered a total of 60-80 credit modules.

Any additional costs

There are no additional costs associated with the programme.

Graduate Attributes, Employability & Personal Development Planning

Graduate Attributes

UWS's Graduate Attributes focus on academic, personal and professional skills and throughout the programmes, 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 are developed throughout and are formalised in 4th year during project studies where School/University ethical approval is sought if required. Links to current University 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 see benefits for our students. The School also runs a number of specific employability events at the Lanarkshire and/or Paisley campuses, including 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 standards: personal tutor support, a number of modules linked to PDP outcomes, support for the development of an e-portfolio, 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: APPD07001 ASPIRE
Second Year: APPD08001 ASPIRE 2 and 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

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.
The sandwich year for MEng students are offered after L9 for full 12 months. A sandwich year is typically assessed through a combination of a written report/ reflective log, and employer evaluation. Based on student's submitted report/portfolio and employer's evaluation, a grade of pass/fail decided. If a student pass this evaluation, the sandwich placement is added in the title, else normal award (BEng or BEng Hons) is provided.

Attendance and Engagement
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.
In alignment with the University's commitment to equality and diversity, this programme actively promotes equal opportunities for students from all backgrounds and with diverse learning needs. Learning materials will be delivered via the Virtual Learning Environment (VLE) in electronic formats that support flexible access and allow for content manipulation to suit individual requirements.

Module coordinators are responsible for ensuring that all University-created materials use inclusive and culturally sensitive language. However, it should be noted that some external resources, such as textbooks or websites, may contain outdated or non-inclusive terminology. Students will be informed of this where applicable.

The programme adheres to the University's regulations and guidance on inclusive learning and teaching practices. Students are encouraged to consult the relevant module coordinator to discuss any specific needs. This will enable appropriate arrangements to be made

regarding assistive technologies, support services, or assessment adjustments, in line with University policies.

Module coordinators will also ensure that all teaching resources are appropriate to the mode of delivery for each module. For laboratory-based modules, where access to physical devices or hardware may not be possible, suitable alternatives such as emulators and virtual software will be provided to ensure that all students have equitable access to essential tools and resources.

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

Learning Outcomes

SCQF LEVEL 7 Learning Outcomes	
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.
A4	
A5	
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.
B4	
B5	
Communication, ICT and Numeracy Skills	
C1	Solve problems of a non-routing nature in creative and innovative ways.
C2	Practice 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	Practice communication skills in electronic as well as written and oral form to a range of audiences.
C5	
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.
D3	
D4	
D5	
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 the society at large.

E2	Manage limited resources within defined areas of computing work.
E3	
E4	
E5	

Level 7 Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
7	COMP07009	Introduction to Web Development	20	☒	☐	☐	
7	COMP07012	CCNA 1: Introduction to Networks	20	☐	☒	☐	
7	COMP07027	Introduction to Programming	20	☒	☒	☐	
7	COMP07086	Fundamentals of Computing System	10	☒	☐	☐	
7	APPD07001	ASPIRE	20	☒	☐	☐	
7	COMP07075	Security Fundamentals	20	☐	☒	☐	
7	MATH07005	Mathematics for Computing	10	☐	☒	☐	
Footnotes for Core Modules COMP07027 runs as a 20 credit module spread over T1 and T2 long and thin.							

Level 7 Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Option Modules							

Level 7 **Criteria for Progression and Award** *Please refer to UWS Regulatory Framework for related regulations*
Award of Certificate of Higher Education (Cert HE) in Computing Science - At least 120 credits at SCQF level 7. 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 90 from the programme are eligible for the exit award of the Certificate of Higher Education in Computing. Distinction will be awarded in line with University Regulations and no imported credit can be used. (Regulations 3.25 & 3.26)

SCQF LEVEL 8 Learning Outcomes	
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.
A5	
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.
B4	
B5	
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 workplace.
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.
C5	
Generic Cognitive Skills - Problem Solving, Analysis, Evaluation	
D1	Employ a range of approaches to formula 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.
D3	
D4	
D5	
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.
E3	
E4	
E5	

Level 8 Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
8	COMP08002	Database Development	20	☒	☐	☐	1
8	COMP08074	Operating Systems	20	☒	☐	☐	
8	COMP08094	Ethical Hacking: Tools & Techniques	20	☐	☒	☐	
8	COMP08100	Linux: Tools and Administration	20	☒	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Core Modules							

Level 8 Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
7	MATH07005	Mathematics for Computing	10	☐	☒	☐	2
7	COMP07027	Introduction to Programming	20	☒	☒	☐	3
8	COMP08101	Programming for Cyber Security	20	☒	☐	☐	3
8	COMP08097	CCNA2 Switching Routing & Wireless Essentials	20	☐	☒	☐	4
9	COMP09115	CCNA1/2: Networks, Routing, Switching & WLANs	30	☒	☒	☐	4
				☐	☐	☐	

Footnotes for Option Modules

1. From 2026/27 year, APPD08001 ASPIRE 2 (T2) will be offered at level 8 in place of COMP08002 Database Development.

2. MATH07005 Mathematics for Computing is offered to direct entry students who have not undertaken any mathematics module at HNC or level 7. This may result in additional credit for direct-entry students.

3. 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. COMP07027 runs as a 20 credit module spread over T1 and T2 long and thin.

4. 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 networking experience.

Level 8
Criteria for Progression and Award
Please refer to UWS Regulatory Framework for related regulations

To progress from SCQF 8 to SCQF 9 in this programme, students are required to obtain 240 credits from the above programme.

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 90 are at SCQF level 8 or above, from the programme are eligible for the exit award of the Diploma of Higher Education in Cyber Security. If a student misses any core module but earns the required credits from other optional modules, they can be awarded Dip HE in Information Technology. Distinction will be awarded in line with University Regulations and no imported credit can be used. (Regulations 3.25 & 3.26)

SCQF LEVEL 9 Learning Outcomes (Maximum of 5 per heading)	
Knowledge and Understanding	
A1	Demonstrate a critical understanding of relevant cyber security principles and practices.
A2	Demonstrate a critical understanding of the scope, main areas and boundaries of cyber security.
A3	Analyse theories, principles, concepts and terminology with cyber security.
A4	
A5	
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.
B4	
B5	
Communication, ICT and Numeracy Skills	
C1	Use a range of tools and techniques associated with cyber security.
C2	
C3	
C4	
C5	
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 judgment in the selection of tools and techniques.
D2	Draw on a range of sources in making judgements.
D3	
D4	
D5	
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.
E3	
E4	
E5	

Level 9 Modules

CORE

SCQF Level	Module Code	Module Title	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	☐	☒	☐	
				☐	☐	☐	
Footnotes for Core Modules							

Level 9 Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
8	COMP08101	Programming for Cyber Security	20	☒	☐	☐	1
9	COMP09115	CCNA1/2: Networks, Routing, Switching & WLANs	30	☒	☒	☐	2
9	COMP09024	Unix System Administrations	20	☒	☐	☐	3
9	COMP09116	CCNA: CyberOps	20	☐	☒	☐	
9	COMP09109	Web Application Security Testing	20	☐	☒	☐	
				☐	☐	☐	

Footnotes for Option Modules

1. COMP08101 Programming for Cyber Security is offered to direct-entry students with no previous programming experience. This may result in additional credit for direct-entry students.

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

3. COMP09024 - Unix System Administration module is only availbale as an option to franchise partners.

Level 9
Criteria for Progression and Award
Please refer to UWS Regulatory Framework for related regulations

To progress from SCQF 9 to SCQF 10 in this programme, students are required to obtain 360 credits, of which 90 credits are at SCQF 9 from the above programme.

Students obtaining 360 credits of which 90 are at SCQF 9 or above from the programme are eligible for the exit award of the BEng Cyber Security.

Distinction will be awarded in line with University Regulations and no imported credit can be used. (Regulations 3.25 & 3.26)

SCQF LEVEL 10 Learning Outcomes (Maximum of 5 per heading**)**	
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, principal 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.
A4	
A5	
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 on 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 a range of the principal skills, practices and/or materials associated within the selected theme(s) of study in a project.
B5	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.

C4	
C5	
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 judgment in the selection of tools and techniques.
D2	Critically review and consolidate knowledge, skills, practices and thinking within the selected theme(s) of study.
D3	Demonstrate originality and creativity in dealing with professional-level computing issues.
D4	
D5	
Autonomy, Accountability and Working with Others	
E1	Practice in ways which show a clear awareness of own and other's roles and responsibilities.
E2	Deal with complex ethical and professional issues in accordance with current professional and/or ethical codes or practices.
E3	
E4	
E5	

Level 10 Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
10	COMP10034	Computing Honours Project	40	☒	☒	☐	
10	COMP10068	Secure Programming	20	☐	☒	☐	
10	COMP10073	Advanced Digital Forensics Analysis	20	☒	☐	☐	
10	COMP10075	Governance, Risk & Compliance	20	☐	☒	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Core Modules							

Level 10 Modules

OPTION

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

10	COMP10014	Network Security	20	☒	☐	☐	COMP10014 or COMP10082
10	COMP10082	Machine Learning for Data Analytics	20	☒	☐	☐	COMP10014 or COMP10082
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
				☐	☐	☐	
Footnotes for Option Modules							

Level 10
Criteria for Progression and Award
Please refer to UWS Regulatory Framework for related regulations

To progress from SCQF 10 to SCQF 11 in this programme, students are normally required to obtain 480 credits from the above programme, with at least 90 credits at SCQF 10.

Students obtaining 480 credits, of which 180 are at SCQF 9 and SCQF 10 (with at least 90 at SCQF 10) from the above programme, including all core modules, but do not satisfy the requirement for progression to Level 11, are eligible for the BEng (Hons) Cyber Security Award.

No Distinction is awarded at the Honours level (Regulation 3.25).

SCQF LEVEL 11 – Integrated Masters Learning Outcomes (Maximum of 5 per heading)	
Knowledge and Understanding	
A1	Demonstrate 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 practice.
A2	Demonstrate 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.
A3	
A4	
A5	
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, conceptualize, analyse and define new and abstract problems given practical constraints.
B4	
B5	
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.
C3	
C4	
C5	
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.
D3	
D4	
D5	
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 ongoing professional development.
E3	Exercise substantial autonomy and initiative in professional and equivalent activities.
E4	
E5	

Level 11 Modules

CORE

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
11	COMP11024	Masters Project	60	☐	☒	☐	
11	COMP11129	IoT Security	10	☒	☐	☐	
11	COMP11090	Malware Analysis & Reverse Engineering	20	☒	☐	☐	
				☐	☐	☐	
				☐	☐	☐	

				☐	☐	☐	
Footnotes for Core Modules							

Level 11 Modules

OPTION

SCQF Level	Module Code	Module Title	Credit	Term			Footnotes
				1	2	3	
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	☐	☒	☐	
Footnotes for Option Modules 30 credits are to be chosen from the following optional modules.							

Level 11
Criteria for Award
Please refer to UWS Regulatory Framework for related regulations

To be eligible for the award of MEng (Honours) Cyber Security 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. Award of distinction and classification is made as per regulations 3.25 and 3.26. 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 a Combined Studies award (please see Regulation 1.61). 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 no: 1

Change/Version Control

What	When	Who
Updated Links: • Academic Engagement Procedure • Equality and Diversity • University Regulatory Framework • Removed invalid links	19/10/2023	C Winter
Guidance Note 2023-24 provided	12/12/2023	D Taylor
General housekeeping to text across sections and addition of links and some specific guidance. Addition of Duration of Study and some other text – for CMA.	12/12/2023	D Taylor
1. Condition of Hons Project for MEng to BEng transferred students removed because Hons Project is added as core for all students. 2. At level 9, wording in the footnote related to optional modules COMP08101 and COMP09110 modified to reflect the actual situation, for example, these modules are offered to students who entered at level 9 with no previous programming experience and may result in additional credit.	21/03/2025	R Singh

3. At level 7, replaced COMP07067 Professional Development in Computing (10 credit) with COMP07086 Fundamentals of Computing System 10 credits T2. 4. At level 7, replaced COMP07061 Computing Systems (20 credits) module with APPD07001 ASPIRE 1 module (20 credits, T1). 5. At level 8, replaced COMP08002 Database Development (20 credits, T1) with APPD08001 ASPIRE 2 (20 credits, T2), w.e.f. from 2026-27 academic year. 6. At level 9, removed MATH07005 Mathematics for Computing, COMP09115 Python for Network Engineers and COMP09086 Information Security Management from options. 7. At level 9, Added a note for COM09024 Unix System Administration that this module is available as an option only to franchise partners. 8. At level 10, replaced COMP10076 Group Research Project (40 credits) with COMP10034 Computing Honours Project (40 credits). 9. At level 11, replaced COMP11093 Mobile Forensics (20 credits, T2) with a new module, COMP11XXX IoT Security (10 credits, T1). 10. At level 11, now 30 credits need to be earned from the pool of optional modules instead of the earlier 20 credits.		