

Undergraduate Programme Specification

Session	2025/26	Last Modified	01/05/2025				
			01/03/2023				
Named Award Title	BEng (Hons) Cyber S	ecurity (Single)					
Award Title for Each	BEng (Hons) Cyber Sec	curity					
Award	BEng Cyber Security						
	Diploma of Higher Edu	cation (DipHE) in Comp	uting				
	Certificate of Higher Ed	ducation (CertHE) in Cor	nputing				
Date of Approval							
Details of Cohort Applies to	From September 2025 the London campus.	From September 2025 for students undertaking this programme at the London campus.					
Awarding Institution	University of the West of Scotland	Teaching University of the West of Scotland					
Language of Instruction	on & Examination	English					
Award Accredited by							
Maximum Period of Ro	egistration	6 Years (Full-time)					
Duration of Study							
Full-time	3 Years	Part-time					
Placement (compulsory)							
Mode of Study	∑ Full-time						
	Part-time						
Campus	Ayr	Lanarkshire	Online / Distance				
	☐ Dumfries	London	Learning				
		Paisley Other (specify)					
School	Computing, Engineering and Physical Sciences						
Divisional Programme Board	Computing						
Programme Leader	Manesh Thankappan						

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:

Standard Entry Requirements: BCCC (90 UCAS Tariff points) including Maths/Applications of Maths or Computing.

Minimum Entry Requirements: CCC (63 UCAS Tariff points) including Maths/Applications of Maths or Computing.

Or GCE

Grades CCD at A-level (88 UCAS Tariff Points), including Maths or Computing at least at GCSE.

Or SQA National Qualifications / Edexcel Foundation

An appropriate HNC/HND award.

Level 8 entry with an HNC with a 'B' in the Graded Unit.

Level 9 entry with at least a 'B' 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

Applicants to the BEng (Hons) Cyber Security programme at UWS will benefit from possessing the following desirable skills and attributes prior to application:

- Basic Programming Knowledge: Familiarity with the use of languages like Python, Java and SQL will be advantageous.
- Mathematical Aptitude: A good foundation in algebra, statistics, or calculus is helpful for understanding key concepts in Cyber Security.
- Analytical Thinking: The ability to approach problems methodically and being able to critically evaluate simulation results or processes.
- Digital Literacy: Comfort with basic computer applications or cloud platforms.
- Communication Skills: Proficiency in written and verbal communication for articulating ideas and collaborating effectively.
- Curiosity and Innovation: A keen interest in technology trends, especially in the advancements in Cyber Security solutions and threats.
- Time Management: Strong organisational skills to manage coursework and independent study effectively.

While not mandatory, these skills will give prospective students a head start in mastering the challenges and opportunities presented in this rapidly evolving field.

General Overview

This programme has been devised to meet a growing need, as identified by the Scottish and UK Governments, for individuals who possess the skillsets to meet the challenges posed by the constantly evolving computer systems.

There is currently a short supply of highly skilled cyber professionals and this programme will produce graduates with the skillsets required to fill this gap. Students will learn to 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-focused programme.

Typical Delivery Method

The BEng (Hons) Cyber Security programme is delivered through a face-to-face teaching mode on campus, offering students a highly interactive and engaging learning experience. Lectures and tutorials are conducted in person, providing opportunities for direct interaction between students and teaching staff. This approach fosters a supportive learning environment where students can easily ask questions, discuss complex concepts, and receive immediate feedback.

To enhance student participation and involvement, a variety of modern educational tools and technologies are integrated into the teaching methodology. These include interactive presentations, group discussions, and live demonstrations of practical techniques. Digital platforms such as MS Teams, Aula, and email communication are utilised to ensure students can access additional support when needed, even outside of formal class hours.

All course materials, including lecture slides, reading resources, and assignments, are made available through the Virtual Learning Environment (VLE), enabling students to review and reinforce their understanding at their own pace. This blended approach ensures students are well-supported both during and outside classroom sessions, promoting active learning and a deeper understanding of core concepts in Cyber Security.

Any additional costs

There are no additional costs associated with this Programme

Graduate Attributes, Employability & Personal Development Planning

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

Critical, analytical and investigative 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. Respectful communication and behaviours are essential.

Ethical awareness and social responsibility are developed throughout and are formalised during the final year project where School/University ethical approval is sought if required.

Links to current University programme research are promoted throughout 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 London campus, including employer speed networking events and an annual 'Working with Industry' event. Guest speakers are invited in the form of industry experts and former students to provide insight.

Personal Development Planning (PDP) within the programme is based on four standards:

- 1) personal tutor support
- 2) numerous modules linked to PDP outcomes
- 3) support for the development of an e-portfolio
- 4) various events relating to PDP

A personal tutor is allocated to 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. These are:

- Level 7: COMP07067 Professional Development in Computing
- Level 8: Embedded in several of the modules
- Level 9: COMP09093 Professional Computing Practice
- Level 10: COMP10034 Computing Honours Project

Work Based Learning/Placement Details

Sandwich placement is not offered as part of this programme.

Attendance and Engagement

In line with the <u>Student Attendance and Engagement Procedure</u>, 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.

For the purposes of this programme, academic engagement equates to the following:

Students are academically engaged if they are regularly attending and participating in timetabled teaching sessions, asynchronous online learning activities, and course-related learning resources, and complete assessments and submit these on time.

Students are also required to be in regular contact with their academic tutor, regularly engaging with materials and discussions on the learning platform, and engaging in independent study.

Equality and Diversity

The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: <u>UWS Equality, Diversity and Human Rights Code.</u>

Aligned with the University's commitment to equality and diversity, this programme supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access to and manipulation of content.

Module Co-ordinators will ensure that language is inclusive and culturally sensitive within any university-created material. However, some external resources, such as textbooks or websites, may still contain outdated or non-inclusive terminology, and students will be made aware of this.

The programme complies with university regulations and guidance on inclusive learning and teaching practice. Students can speak to the the relevant Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.

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.
А3	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).
В3	Employ the professional skills, techniques, practices and/or materials associated with cyber security.
В4	
В5	
	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, adjusting features to suit the purpose.
C4	Practice electronic, oral and written communication skills suitable for their target audience.
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 society at large.

E2	Manage limited resources within defined areas of computing work.
E3	
E4	
E 5	

Level 7 Modules

CORE

SCQF	Module	Module Title	Credit	Terr	n		Footnotes
Level	Code			1	2	3	
7	COMP07009	Introduction to Web Development	20				
7	COMP07012	CCNA 1: Introduction to Networks	20				
7	COMP07027	Introduction to Programming	20	\boxtimes		\boxtimes	
7	COMP07086	Fundamentals of Computing Systems	10				
7	APPD07001	Aspire: Foundations For Success	20				
7	COMP07075	Security Fundamentals	20	\boxtimes		\boxtimes	
7	MATH07005	Mathematics for Computing	10				

Footnotes for Core Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake.

Student entry point determines the relevant module delivery for initial and subsequent term modules. Students will undertake either Module Group 1 or Module Group 2 on their initial Term, and complete the other Module Group in the following Term. This will be communicated and explained during programme induction and programme material provided.

Module group 1: Introduction to Web Development; Aspire: Foundations For Success, and Mathematics for Computing and Fundamentals of Computing Systems; OR

Module group 2: CCNA1: Introduction to Networks; Introduction to Programming and Security Fundamentals.

Level 7 Modules

OPTION

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

Footno	tes for Option	Modules			
Level					
	•	ion and Award			
Please	refer to <u>UWS</u>	Regulatory Fram	<u>ework</u> for related re	gulations	
	the Regulator 40-credit defic		udents are eligible t	o progress from I	Level 7 to Level 8
To be eligible for the award of Certificate of Higher Education (CertHE) Computing, a student must comply with the UWS Regulatory Framework: students must achieve 120 credit points at SCQF level 7. Students must also successfully pass all core modules for this exit award.					

	SCQF LEVEL 8
	Learning Outcomes
	Knowledge and Understanding
44	
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.
В3	Analyse a new or existing workplace system, designing and implementing a relational database to better meet client 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, using a range of standard applications to process and obtain data.
СЗ	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 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.
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	Module	Module Title	Credit	Term			Footnotes
Level	Code			1	2	3	
8	APPD08001	Aspire: Shaping Your Future	20	\boxtimes	\boxtimes	\boxtimes	
8	COMP08074	Operating Systems	20	\boxtimes	\boxtimes	\boxtimes	
8	COMP08094	Ethical Hacking: Tools & Techniques	20				
8	COMP08100	Linux: Tools and Administration	20		\boxtimes	\boxtimes	

Footnotes for Core Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake.

Student entry point determines the relevant module delivery for initial and subsequent term modules. Students will undertake either Module Group 1 or Module Group 2 on their initial Term, and complete the other Module Group in the following Term. This will be communicated and explained during programme induction and programme material provided.

Module group 1: Operating Systems; Ethical Hacking: Tools & Techniques

Module group 2: Aspire: Shaping Your Future; Linux: Tools and Administration

Level 8 Modules

OPTION

SCQF	Module	Module Title	Credit	Term			Footnotes
Level	Code			1	2	3	
8	COMP08101	Programming for Cyber Security	20	\boxtimes	\boxtimes	\boxtimes	
8	COMP08097	CCNA2 Switching Routing & Wireless Essentials	20				

Footnotes for Option Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake. Student entry point determines the module delivery of initial Term and second Term modules.

Students will undertake either Module 1 or Module 2 on their initial Term, and complete the other Module Group in the following Term. Where this will be communicated and explained during programme induction and programme material provided.

Module 1: CCNA2: Switching Routing & Wireless Essentials

Module 2: Programming for Cyber Security

Level 8

Criteria for Progression and Award

Please refer to <u>UWS Regulatory Framework</u> for related regulations

Within the Regulatory Framework, students are eligible to progress from Level 8 to Level 9 with 40-credit deficit.

To be eligible for the award of Diploma of Higher Education (DipHE) in Computing, a student must comply with the Regulatory Framework: students must achieve 240 credits points of which a minimum of 90 are at SCQF Level 8 or above. Students must also successfully pass all core modules for this exit award.

SCQF LEVEL 9 Learning Outcomes (Maximum of 5 per heading) **Knowledge and Understanding** Α1 Demonstrate a critical understanding of relevant cyber security principles and practices. Demonstrate a critical understanding of the scope, main areas and boundaries of cyber **A2** А3 Analyse theories, principles, concepts and terminology with cyber security. Α4 Α5 **Practice - Applied Knowledge and Understanding** Practice routine methods of enquiry and research associated with computing science. В1 Apply the principal skills, techniques, practices and/or materials associated with cyber **B2** 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 application of computer technology, and be guided by the adoption of appropriate professional, ethical and legal practices in the workplace. **E2** Use initiative in managing ethical and professional issues in accordance with current professional and/or ethical codes or practices. **E3 E4 E**5

Level 9 Modules

CORE

SCQF	Module	Module Title	Credit	Terr	n		Footnotes
Level	Code			1	2	3	
9	COMP09092	Research Methods in Computing	10				
9	COMP09093	Professional Computing Practice	10				
9	COMP09106	Cryptography	20	\boxtimes	\boxtimes	\boxtimes	
9	COMP09107	Digital Forensic Analysis	20		\boxtimes	\boxtimes	
9	COMP09111	Systems Programming Concepts	20				

Footnotes for Core Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake.

Student entry point determines the relevant module delivery for initial and subsequent term modules. Students will undertake either Module Group 1 or Module Group 2 on their initial Term, and complete the other Module Group in the following Term. This will be communicated and explained during programme induction and programme material provided.

Module group 1: Cryptography; Digital Forensic Analysis; System Programming Concepts

Module group 2: Research Methods in Computing; Professional Computing Practice

Level 9 Modules

OPTION

SCQF	Module	Module Title	Credit	Term		Footnotes	
Level	Code			1	2	3	
9	COMP09109	Web Application Security Testing	20				
9	COMP09116	CCNA: CyberOps	20	\boxtimes		\boxtimes	

Footnotes for Option Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake.

Student entry point determines the module delivery of initial Term and second Term modules. Students will undertake both modules on their respective Term where this will be communicated and explained during programme induction and programme material provided.

Level 9		
Criteria fo	r Progression and	l Award

Please refer to <u>UWS Regulatory Framework</u> for related regulations

Within the Regulatory Framework, students are eligible to progress from Level 9 to Level 10 with 20-credit deficit.

To be eligible for the award of BEng Cyber Security students must comply with the Regulatory Framework: students must achieve 360 credits points of which a minimum of 90 are at SCQF Level 9 or above. Students must also successfully pass all core modules for this exit award.

	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.					
А3	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.					
В3	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.					
B5						
	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.
E 3	
E4	
E 5	

Level 10 Modules

CORE

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

Footnotes for Core Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake.

Student entry point determines the module delivery of initial Term and second Term modules. Students will undertake either Module Group 1 or Module Group 2 on their initial Term, and complete the other Module Group in the following Term. Where this will be communicated and explained during programme induction and programme material provided.

Module group 1: Secure Programming; Advanced Digital Forensics Analysis; Governance, Risk & Compliance

Module group 2: Computing Honours Project	

Level 10 Modules

OPTION

SCQF	Module	Module Title	Credit	Term		Footnotes	
Level	Code			1	2	3	
10	COMP10014	Network Security	20	\boxtimes	\boxtimes	\boxtimes	
		OR					
10	COMP10082	Machine Learning for Data Analytics	20		\boxtimes		

Footnotes for Option Modules

The delivery format on London campus is cyclic, based on 3 term delivery and student intake.

Student entry point determines the module delivery of initial Term and second Term modules. Students will undertake both modules on their respective Term where this will be communicated and explained during programme induction and programme material provided.

Select ONE module (20 credits) from the list. Optional modules available are dependent on the number of students enrolled on module. This will be discussed and explained with the Programme Team.

Level 10

Criteria for Award

Please refer to <u>UWS Regulatory Framework</u> for related regulations

To be eligible for the award of BEng (Hons) Cyber Security students must comply with the Regulatory Framework: students must achieve 480 credits points of which a minimum of 90 are at SCQF Level 10 or above. Students must undertake an independent dissertation element and also successfully pass all core modules for this exit award.

Regulations of Assessment

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

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
To align with the BEng Cyber	01-05-2025	Manesh Thankappan
Security delivery at the		
Paisley campus, this		
Programme Specification has		
been updated at Levels 7 and		
8 to reflect the inclusion of		
the ASPIRE modules.		
Changes at Level 7:		
1.Professional Development		
in Computing (COMP07067)		
has been removed and		
replaced with ASPIRE		
module (APPD07001).		
2.Computing Systems		
(COMP07061) has been		
removed and replaced with		
Fundamentals of Computing		
Systems (COMP07086).		
Changes at Level 8:		
1.Database Development		
(COMP08002) has been		
removed and replaced with		
ASPIRE module		
(APPD08001).		