Programme Specification

Cyber Security and Networking [UCW]

Version: 2025-26, v1.0, 20 Jan 2025

Contents

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Cyber Security and Networking [UCW]

Highest award: FdSc Cyber Security and Networking

Interim award: CertHE Cyber Security and Networking

Awarding institution: UWE Bristol

Affiliated institutions: University Centre Weston

Teaching institutions: University Centre Weston

Study abroad: No

Year abroad: No

Sandwich year: No

Credit recognition: No

School responsible for the programme: CATE School of Computing and Creative Technologies, College of Arts, Technology and Environment

Professional, statutory or regulatory bodies: Not applicable

Modes of delivery: Full-time

Entry requirements:

For implementation from: 01 September 2025

Programme code: I10L00

Section 2: Programme Overview, Aims and Learning Outcomes

Part A: Programme Overview, Aims and Learning Outcomes

Overview: The FdSc Cyber Security and Networking has been developed in partnership with employers, reflecting local and national demand for Cyber Security professionals. This programme has been mapped to the IfA HTQ ST1021 standard (Cyber Security Technologist).

Cyber Security Technologists all require an understanding of security concepts and technology and how to mitigate risks arising from threats. The specific tasks undertaken vary depending on what needs to be achieved by the team at any particular time. Some tasks may be very technical, others may be more analytical, business or user focused. All roles in this occupation work to achieve required cyber security outcomes in a legal and regulatory context in all parts of the economy. They develop and apply practical knowledge of information security to deliver solutions that fulfil an organisations requirement.

The broad purpose of the occupation is to apply an understanding of cyber security to protect organisations, systems, information, personal data and people from attacks and unauthorised access.

Features of the programme:

Educational Aims: This programme will:

Foster in students innovation, enterprise and enthusiasm for excellence in computing.

Develop students' technical skills so they can make an effective and professional contribution to the work of interdisciplinary groups engaged in computing projects.

Develop security designs with design justification to meet the defined cyber security parameters.

Configure, deploy and use computer, digital network and cyber security technology.

Keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development.

Develop program code or scripts for a computer or other digital technology for example, an industrial control system.

Demonstrate and apply effective workplace skills such as: innovation and creativity; self-management; self-awareness and reflection; goal setting and action planning; independence and adaptability; communication skills; acting on initiative; innovation and creativity, for the benefit of both personal and organisational development.

Develop personal study, communication, presentation and interpersonal skills required for both independent, autonomous practice and teamworking.

Develop analytical problem-based learning skills and the transferable skills to prepare students for employment and continuing professional development leading to a lifelong learning approach.

Enable students to demonstrate sound knowledge of the concepts, principles and practice from a range of discipline areas within the computing field.

Analyse test objectives to design and prepare a test plan that aligns with the test strategy

Programme Learning Outcomes:

On successful completion of this programme graduates will achieve the following learning outcomes.

Programme Learning Outcomes

PO1. Identify security threats and hazards to a system, service or processes to inform risk assessments and design of security features

PO2. Apply problem-solving techniques to analyse, evaluate and address cyber security threats to technology solutions and implement mitigation through technical and process solutions.

PO3. Plan, design and manage computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context.

PO4. Configure, deploy and use computer, digital network and cyber security technology.

PO5. Analyse the extent to which a computer-based system meets the criteria defined for its current use and future development.

PO6. Develop practical data solutions to securely store, manage data structures and present data to provide new business insight.

PO7. Keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development

PO8. Manage cyber security operations processes in accordance with organisational policies and standards and business requirements.

Assessment strategy: Throughout the programme, opportunities for formative assessment will support summative assessment. A variety of assessment methods will be used including: presentations; reports; coursework, professional briefs and projects, with an emphasis on practical, industry derived skills to give students to demonstrate their proficiency and practical skills across specialist modules.

Students will be assessed using scenarios that require problem solving, working both individually and as part of a team. Assessment will develop from module activity, including formative assessment, to ensure that students are fully supported. The assessments provide appropriate challenges to engage students with academic, research, and work-based opportunities to support their developing professionalism.

The assessment of practical system developments and programming skills is embedded throughout the programme. As students progress through the programme, project management, development and collaboration become a key theme, and is seen as core activity within the computing industries.

Opportunities for formative feedback are utilised via practical tasks, labs and mock assessments to give students the best opportunity to prepare for summative assessments.

Student support: Personal Development, including academic writing and research skills are delivered through the Academic Development Team, which is embedded in the tutorial programme.

In addition, students may be able to participate in wider opportunities available across the institution. Note: Extra-curricular trips may require student contribution to all or some of the costs and are offered subject to availability and demand.

Part B: Programme Structure

Year 1

Students must take 120 credits from the modules in Year 1.

Year 1 Compulsory Modules

Students must take 120 credits from the modules in Compulsory Modules.

Module Code	Module Title	Credit
UFCFSM-15-1	Business Security 2025-26	15
UFCE4N-15-1	Computer Networks and Protocols 2025-26	15
UFC4EP-15-1	Database Development 2025-26	15
UFCFQM-30-1	Fundamentals of Software Development 2025-26	30
UFCEHX-15-1	Operating Systems and Networks 2025-26	15
UFCFRE-30-1	Web Technologies and Platforms 2025-26	30

Year 2

Students must take 120 credits from the modules in Year 2.

Year 2 Compulsory Modules
Students must take 120 credits from the modules in Compulsory modules.

Module Code	Module Title	Credit
UFCEHV-15-2	Cyber Threat Analysis 2026-27	15
UFCE53-30-2	Cyber Security Forensics 2026-27	30
UFCEHT-30-2	Introduction to Ethical AI 2026-27	30
UFCF9R-15-2	Project Management 2026-27	15
UFCF8R-30-2	Webapp Development 2026-27	30

Part C: Higher Education Achievement Record (HEAR) Synopsis

Computer development and digital applications evolve rapidly within the technology industries, but the fundamental knowledge and skills that enable their development, remains the same. For this reason, skill development, theoretical knowledge and the application of underpin the programme.

Alongside both skill and digital knowledge, application and understanding; students are actively encouraged to pursue personal career ambitions; not just for industry employment, but to develop life long learning, financial sustainability and industry engagement.

Part D: External Reference Points and Benchmarks

There are no PSRB requirements for this programme. This programme has been designed to embed the principles, knowledge, application and skills outlined in the UK Quality Code for Higher Education's Subject Benchmark Statement for Computing (March 2022). Furthermore, this programme has also been aligned to the Higher Technical Qualification (HTQ) Cyber Security Technologist standard ST1021 (subject to approval)

Part E: Regulations

Approved to University Regulations and Procedures