Programme Specification

Cyber Security and Networking {Top-up} [UCW]

Version: 2027-28, v1.0, 20 Jan 2025

Contents

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Cyber Security and Networking {Top-up} [UCW]

Highest award: BSc (Hons) Cyber Security and Networking

Interim award: BSc 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 2027

Programme code: I10M00

Section 2: Programme Overview, Aims and Learning Outcomes

Part A: Programme Overview, Aims and Learning Outcomes

Overview: The BSc (Hons) Cyber Security and Networking has been developed in partnership with employers, reflecting local and national demand for cyber security and networking professionals.

Cyber security and networking 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 and networking 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 specifically aims to:

Foster innovation, enterprise and enthusiasm for excellence in cyber security and networking.

Develop technical skills leading to an effective and professional contribution to the work of interdisciplinary groups engaged in cyber security projects.

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

Develop software solutions to meet professional requirements using a range of languages and software tools.

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 for employment and continuing professional development leading to a lifelong learning approach.

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

Programme Learning Outcomes:

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

Programme Learning Outcomes

PO1. Demonstrate professional use of research methods to select and specify appropriate technology solutions, including the analysis of ethical and legal implications.

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

PO3. Critically evaluate and manage complex computer networks focussing on the services and capabilities that network infrastructure solutions enable, including analysing and assessing network security risks, information security and compliance.

PO4. Select, configure and deploy enterprise, digital network and cyber security infrastructure.

PO5. Effectively design and deploy innovative solutions to develop IT infrastructure within complex organisations, utilising tools for the construction and documentation of computer appliances.

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

The assessment of practical system developments and programming skills is embedded throughout the programme. Project management, development and collaboration are key themes, and are seen as core activities 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 level appropriate academic writing and research skills are delivered through the Academic Development Team, which is embedded in the tutorial programme.

Students are supported by the careers advice service to plan their future professional development.

In addition, students may have opportunities 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 in Year 1

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

Module Code	Module Title	Credit
UFCEJ5-30-3	Directory Services and Policy Management 2027-28	30
UFCFEN-15-3	Cloud Computing Platforms 2027-28	15
UFCFET-15-3	Research & Emerging Technologies 2027-28	15
UFCFBR-30-3	Internet of Things (IoT) 2027-28	30
UFCE59-30-3	Network Infrastructure Planning 2027-28	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).

Part E: Regulations

Approved to University Regulations and Procedures