Programme Specification

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl]

Version: 2022-23, v0,

Contents

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl]

Highest award: BSc (Hons) Cyber Security Technical Professional

Interim award: BSc Cyber Security Technical Professional

Interim award: DipHE Cyber Security Technical Professional

Interim award: CertHE Cyber Security Technical Professional

Awarding institution: UWE Bristol

Affiliated institutions: Gloucestershire College

Teaching institutions: Gloucestershire College

Study abroad: Yes

Year abroad: No

Sandwich year: No

Credit recognition: No

Department responsible for the programme: Z-FET Dept of Computer Sci & Creative Tech, Z-FET_CMT Restructure

Contributing departments: Not applicable

Professional, statutory or regulatory bodies: Not applicable

Apprenticeship: ST0409

Mode of delivery: Full-time

Entry requirements: The University's Standard Entry Requirements apply with the following additions:

Individual employers will set the selection criteria

Tariff points as appropriate for the year of entry - up to date requirements are available through the UWE Bristol website.”

For implementation from: 21 September 2020

Programme code: I99100

Section 2: Programme Overview, Aims and Learning Outcomes

Part A: Programme Overview, Aims and Learning Outcomes

Overview: The BSC (Hons) Cyber Security Technical Professional (integrated degree) programme is aligned to the Institute for Apprenticeships and Technical Education standard.

Graduates of the programme will have knowledge skills within the area of cyber security. Their knowledge will have been build through sound, classroom-based pedagogy integrated with practical experience gained through their employment.

As an apprenticeship programme, it is by its very nature practice-led. It is inter-disciplinary in the Cyber Security cuts across almost all disciplines and students will be exposed to the issues as they affect a range of disciplines including critical national infrastructure, transport, finance, public and private sector functions.

When they graduate from this programme, students will be able to operate with a considerable degree of autonomy and lead   teams which   research, analyse, model, assess and manage cyber security risks. They will be able to work-ready and will act in accordance with applicable laws, regulations, standards and ethics.

Educational Aims: The BSC (Hons) Cyber Security Technical Professional (integrated degree) programme has the following general aims and is aligned to the Institute for Apprenticeships and Technical Education standard:

•To enable apprentices to operate in business or technology / engineering functions across a range of sectors of the economy including critical national infrastructure (such as energy, transport, water, finance), public and private, large and small.

•To enable apprentices to operate with a considerable degree of autonomy and lead teams which:

oresearch, analyse, model, assess and manage cyber security risks

odesign, develop, justify, manage and operate secure solutions

odetect and respond to incidents

•To allow them to work in accordance with applicable laws, regulations, standards and ethics.

The cyber security technical professional (integrated degree) has the following specific aims:

•To provide the technical knowledge and understanding of:

oFoundations of cyber security

oFoundations of networking

oInformation management

oComputer architecture and operating systems

oSecure software development and cryptography

oThreats, risk analysis and mitigation

oSecure system design

oSecurity cases and assurance

oThe legal, regulatory and ethical environment and responsibilities

•To develop both personal and inter-personal skills to enable apprentices to work effectively with others

•To provide apprentices with a set of problem-solving, analytical and critical thinking skills for technology solutions development,

•To develop the ability to propose, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business needs

•To encourage apprentices to demonstrate business disciplines, ethics and courtesies, demonstrating timeliness and focus when completing tasks to a deadline with high quality

Modules will be based on ensuring that apprentice’s practical skills and knowledge gained in the taught sessions are carried into the workplace to inform their employment and generation of evidence of competency.

Note: Team working, management and problem solving skills will be developed in the workplace and specifically assessed as competencies in the end point assessment.

Programme Learning Outcomes:
On successful completion of this programme graduates will achieve the following learning outcomes.

Programme Learning Outcomes

PO1. Demonstrate a detailed understanding of the architecture, implementation and operation of computer systems and embedded devices

PO2. Design and implement secure networks using the appropriate technology, embedded devices and protocols

PO3. Apply programming principles and levels of abstraction to provide secure solutions for systems and applications.

PO4. Recognise the context in which cyber threats exist, their methods and harm.

PO5. Apply knowledge of secure and cryptographic methods to protect systems

PO6. Demonstrate knowledge and understanding of information management, computing services and distributed data systems

PO7. Assess risk, assure systems, analyse malware and manage cyber incidents

PO8. Apply their understanding of the social, legal, ethical, economic, managerial and professional issues relating to cyber security practice

Part B: Programme Structure

Year 1

Year 1 is a full time delivery taught at Gloucestershire College.

Module Code	Module Title	Credit
UFCFFU-30-1	Cyber Threats 2022-23	30

UFCFDU-30-1	Networking 2022-23	30
UFCFCU-30-1	Operating Systems and Architecture 2022-23	30
UFCFEU-30-1	Programming 2022-23	30

Year 2

Year 2 is a full time delivery taught at Gloucestershire College.

Module Code	**Module Title**	**Credit**
UFCFGU-30-2	Cryptography 2023-24	30
UFCFJU-30-2	Embedded Systems Security 2023-24	30
UFCFKU-30-2	Information management and security 2023-24	30
UFCFHU-30-2	Operating Systems Security and Defensive Programming 2023-24	30

Year 3

Year 3 is a full time delivery taught at UWE Bristol.

Module Code	**Module Title**	**Credit**
UFCFNU-20-3	Cyber Security Incident Management and Professionalism 2024-25	20
UFCFBU-10-3	End Point Assessment (Cyber Security) 2024-25	10
UFCFPU-30-3	Project and Dissertation 2024-25	30
UFCFMU-30-3	Risk and Information Management 2024-25	30
UFCFLU-30-3	Security Assurance 2024-25	30

Part C: Higher Education Achievement Record (HEAR) Synopsis

BSc (Hons) Cyber Security Technical Professional (integrated degree) provides apprentices with the skills and capabilities required by businesses for research, analysis, modelling, assessment and management of cyber security risks. They can design, develop, justify, manage and operate secure solutions; and detect and respond to incidents. They work to applicable laws, regulations, standards and ethics. It develops technically competent individuals who think and communicate effectively and who can conduct inquiry, solve problems, undertake critical analysis and deliver effective solutions in a constantly changing business context.

It provides a solid foundation for lifelong learning, emphasising the development of knowledge, skills and values essential to a cyber security professional.

Part D: External Reference Points and Benchmarks

The following reference points and benchmarks have been used in the in the design of the programme:

Institute for Apprenticeships Cyber Security Technical Professional (Integrated Degree) standard.
Institute for Apprenticeships Cyber Security Technical Professional (Integrated Degree) assessment plan.
National Cyber Security Centre Certification of Degree Apprenticeships in Cyber Security (2019)

The Subject Benchmarking Statements for the computing field (https://www.qaa.ac.uk/docs/qaa/subject-benchmark-statements/sbs-computing-16.pdf?sfvrsn=26e1f781_12) were consulted in designing this programme. The skills recommended for computing students cover three broad categories:
computing-related cognitive skills,
computing-related practical skills
generic skills for employability.
The statements do not explicitly reference cyber security.

The design of the programme has ensured that the skills specified for each category (and relevant to this programme) are incorporated within the modules for the programme.

QAA UK Quality Code for HE
Framework for higher education qualifications (FHEQ) was consulted to ensure that that module level outcomes are appropriate to agreed national standards.

The practice-led, partnership based nature of this programme is consistent with UWE's strategy 2030.

Part E: Regulations

Approved to University Regulations and Procedures.