SECTION 1: KEY PROGRAMME DETAILS

PART A: PROGRAMME INFORMATION	
Highest Award	BSc (Hons) BSc (Hons) Cyber Security Technical Professional (integrated degree)

Awarding Institution	UWE Bristol
Teaching Institution	Gloucestershire College
Delivery Location	Gloucester Campus
Study Abroad / Exchange / Credit Recognition	Placement ✓ Sandwich Year X Credit Recognition X Year Abroad X
Faculty Responsible For Programme	Faculty of Environment & Technology
Department Responsible For Programme	FET Dept of Computer Sci & Creative Tech
Apprenticeships	ST0409
Mode of Delivery	Part-time

ENTRY REQUIREMENTS	UCAS Tariff Points: 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 Sep 2020
ISIS Code/s	Programme Code Other codes: JACS Computer science HECoS 100366: Computer Science

	UCAS SLC

SECTION 2: PROGRAMME OVERVIEW, AIMS and LEARNING OUTCOMES

PART A: PROGRAMME OVERVIEW, AIMS and LEARNING OUTCOMES

1. (Programme) Overview (c. 400 words)

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.

2. Educational Aims (c. 4-6 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:
  - research, analyse, model, assess and manage cyber security risks
  - design, develop, justify, manage and operate secure solutions
  - detect 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:
  - Foundations of cyber security
  - Foundations of networking
  - Information management
  - Computer architecture and operating systems
  - Secure software development and cryptography
  - Threats, risk analysis and mitigation
  - Secure system design
  - Security cases and assurance
  - The 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,

PART A: PROGRAMME OVERVIEW, AIMS and LEARNING OUTCOMES

• 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.

3. Programme and Stage Learning Outcomes (c. 6-8 outcomes)

Programme (Learning) Outcomes (POs)

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

1. Structure

Year 1

Code	Module Title	Credit	Type
UFCFFU-30-1	Cyber Threats 2020-21	30	Compulsory
UFCFDU-30-1	Networking 2020-21	30	Compulsory
UFCFCU-30-1	Operating Systems and Architecture 2020-21	30	Compulsory
UFCFEU-30-1	Programming 2020-21	30	Compulsory

Year 2

Code	Module Title	Credit	Type
UFCFGU-30-2	Cryptography 2021-22	30	Compulsory
UFCFJU-30-2	Embedded Systems Security 2021-22	30	Compulsory
UFCFKU-30-2	Information management and security 2021-22	30	Compulsory
UFCFHU-30-2	Operating Systems Security and Defensive Programming 2021-22	30	Compulsory

Year 3

Code	Module Title	Credit	Type
UFCFNU-20-3	Cyber Security Incident Management and Professionalism 2022-23	20	Compulsory
UFCFBU-10-3	End Point Assessment (Cyber Security) 2022-23	10	Compulsory
UFCFPU-30-3	Project and Dissertation 2022-23	30	Compulsory
UFCFMU-30-3	Risk and Information Management 2022-23	30	Compulsory
UFCFLU-30-3	Security Assurance 2022-23	30	Compulsory

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