SECTION 1: KEY PROGRAMME DETAILS

PART A: PROGRAMME INFORMATION	
Highest Award	MSc Cyber Security
Interim Award	PGCert Cyber Security
Interim Award	PGDip Cyber Security

Awarding Institution	UWE Bristol
Teaching Institution	UWE Bristol
Delivery Location	Frenchay Campus
Study Abroad / Exchange / Credit Recognition	Placement X 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
Professional Statutory or Regulatory Body (PSRB) Links	National Cyber Security Centre (NCSC)
Apprenticeships	
Mode of Delivery	Part-time

ENTRY REQUIREMENTS	UCAS Tariff Points: For the current entry requirements see the UWE public website.
For Implementation From	1 Sep 2020
ISIS Code/s	Programme Code I900-SEP-PT-FR-I900

	Other codes: JACS Others in Computer sciences HECoS 100000: Undefined UCAS SLC

SECTION 2: PROGRAMME OVERVIEW, AIMS and LEARNING OUTCOMES

PART A: PROGRAMME OVERVIEW, AIMS and LEARNING OUTCOMES

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

This MSc Cyber Security programme is aimed at graduates of computing based degrees; for example, Computer Science, Cyber Security, Information Security, who wish to develop their knowledge, understanding, and skills in the general aspects of Cyber Security. The programme will provide them with a common foundation, which then forms the basis for the study of various aspects and technologies of secure systems.

Graduates of this programme will typically have the appropriate knowledge and skills to undertake senior technical roles within Cyber Security.

2. Educational Aims (c. 4-6 aims)

The programme develops underpinning knowledge and skills in fundamental areas such as computer and network security and parallel computing. Parallel computing is particularly relevant in cyber security as it is used when handling large amounts of data and also when running complex algorithms over significantly large data sets.

Students further develop their knowledge and skills, studying various aspects and technologies within the cyber security domain; for example: cryptography as applied to cyber security, the security of IOT and critical systems.

Students will study information security management and information risk management (placing these within a legal context).

Additionally, students will develop their knowledge and understanding of current issues and research within the cyber security domain, and develop research skills in preparation for their dissertation. Within the dissertation, students will identify and research a topic relevant to the cyber security domain.

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

PART A: PROGRAMME OVERVIEW, AIMS and LEARNING OUTCOMES

Programme (Learning) Outcomes (POs)

Knowledge and Understanding

A1	Deep and systematic knowledge and understanding of the concepts and technologies used to establish and maintain computer and network security
A2	Understand how current methodological approaches and legal frameworks influence the role of information security management and information risk management
A3	Understand the complexities of contemporary computer systems and the challenges they present to cyber security
A4	Emerging methods and technologies within the cyber security arena; both in terms of threat vectors and counter measures

Intellectual Skills

B1	Use appropriate models to evaluate threats to cyber security
B2	Synthesize resources from a range of disciplines to provoke original thinking about aspects cyber security
B3	Develop critical responses to existing issues in cyber security and suggest future directions

Subject/Professional Practice Skills

C1	Design security solutions taking into account the changing landscape of threats and vulnerabilities
C2	Implement demonstrably reliable and robust security solutions
C3	Manage and evaluate security aspects of digital systems

Transferable Skills and other attributes

D1	Communicate ideas, arguments and information in a clear, effective and reasoned way in both individual and group situations
D2	Respond resourcefully and creatively to challenges
D3	Effectively plan and manage projects including managing one’s own time
D4	Use personal reflection effectively to analyse self and own actions to inform decision making
D5	Take account of the ethical dimensions of one’s practice, managing the implications of ethical dilemmas and working proactively with others to formulate solutions

PART B: Programme Structure

1. Structure

Year 1

Year 1 Compulsory Modules

Code	Module Title	Credit	Type
UFCFVN-30-M	Computer and Network Security 2020-21	30	Compulsory
UFCFWN-15-M	Information Risk Management 2020-21	15	Compulsory
UFCFFL-15-M	Parallel Computing 2020-21	15	Compulsory

Year 2

Year 2 Compulsory Modules

Code	Module Title	Credit	Type
UFCFYN-15-M	Analysis and Verification of Concurrent Systems 2021-22	15	Compulsory
UFCF7P-15-M	Critical Systems Security 2021-22	15	Compulsory
UFCF9Y-60-M	CSCT Masters Project 2021-22	60	Compulsory
UFCFXN-15-M	Cyber Security Futures Emerging Trends and Challenges 2021-22	15	Compulsory
UFCF8P-15-M	IoT Systems Security 2021-22	15	Compulsory

PART C: Higher Education Achievement Record (HEAR) Synopsis

On successful completion of this programme, graduates will have the appropriate knowledge, skills, and understanding to work at a senior technical level in the security domain of complex computer systems as well as roles in Information Security Consultant, Security Auditor etc. They will have a detailed

PART C: Higher Education Achievement Record (HEAR) Synopsis

understanding of computer and networks security and the context in which complex computer systems operate, including relevant legislation and standards. They will have specialised knowledge of the technologies associated with complex secure systems (including industrial control systems and the Internet of Things), and the verification and testing of such systems.

PART D: EXTERNAL REFERENCE POINTS AND BENCHMARKS

In designing this programme, the following external reference points and benchmarks have been used:

QAA UK Quality Code for HE

NCSC – National Cyber Security Centre guidelines/requirements.

National qualification framework

Subject benchmark statement - Masters in Computing

QAA Master's degree characteristics

University strategies and policies

Industry consultation and external academic advice

The design of this programme and its associated module specifications aims to address skills shortages within the cyber security industry in the UK and, in particular, the South West and surrounding areas corridor. This shortage has been identified as a significant barrier to growth within industry reports ((ISC)2, NCSC), PSRB educational advisor / external academics, and range of industry professionals and collaborators.

The UK and global skills gap in cyber security are widely acknowledged. (ISC)2, the security certification and industry body, predicts that companies and public sector organisations will need 6m security professionals by 2019 but only 4.5m will have the necessary qualifications. In addressing this skills gap, the NCSC has a remit to nurture and grow the UK's national cyber security capability; their academic accreditation scheme is one aspect of their strategy to achieve this. Getting the programme approved and professionally certified by the National Cyber Security Centre (NCSC) is crucial as evidence to the new cohort that UWE is delivering a recognised programme delivered by a fully qualified and endorsed team.

This will align to UWE vision 2020 in encouraging and attracting more postgraduate students into education as another route for employment and skills development. UWE currently provides a BSc (Hons) Forensic Computing and Security programme. Feedback from students on this programme indicates that they would like the opportunity to further develop their skills in cyber security, either on a full-time or parttime basis. There has also been steady interest from UWE students, on other degree programmes, into the field of cyber security.

The programme structure and design are informed by QAA and NCSC recommendations incorporating a range of learning, teaching and assessment methods to prepare students for immediate entry into further study or employment. Aims and learning outcomes of the programme and modules have been explicitly designed to align with Master's level study as defined within the FHEQ / SEEC descriptors and the QAA qualification characteristics for Master's degrees, matching vocabulary where possible to make these links particularly clear.

For NCSC requirements and benchmark: For General cyber security the MSc needs to demonstrate that a minimum of 70% of the taught credits are in cyber security and these can be mapped to any of Security Disciplines A to H. This has been met and demonstrated in table 3.1 of section 3 of the application for professional certifications. We use these Security Disciplines as a benchmark to justify the MSc modules

PART D: EXTERNAL REFERENCE POINTS AND BENCHMARKS
are within the scope of cyber security, as the requirement for NCSC we have made sure that 70% of taught credits have been mapped to at least one of these Security Disciplines. The module specifications have also demonstrated that the taught modules and assessments cover at least 9 of the 13 Skills Groups in good breadth and depth.

PART E: REGULATIONS
Approved to University Regulations and Procedures