Bournemouth University

KEY PROGRAMME INFORMATION

Originating institution(s) Bournemouth University	**Faculty responsible for the programme** Faculty of Science and Technology
Final award(s), title(s) and credits MSc Cyber Security & Human Factors - 180 Credits (90 ECTS)	
Intermediate award(s), title(s) and credits PGDip Cyber Security & Human Factors- 120 Credits (60 ECTS) PGCert Computing - 60 Credits (30 ECTS)	
UCAS Programme Code(s) (where applicable and if known) N/A	**HECoS codes** 100376 – Computer and Information Security (major), 100736 – Human Factors (major) 100373 - Internet Technologies (minor)
External reference points • www.cphc.ac.uk/docs/cphc_masters_april_final.pdf http://www.qaa.ac.uk/academicinfrastructure/fheq/EWNI/default.asp QAA Chapter A1: The national level (incorporating the Framework for Higher Education Qualifications (FHEQ) in England, Wales and Northern Ireland) QAA Chapter A2: The Subject and Qualification Level (incorporating Masters Degree Characteristics)	
Professional, Statutory and Regulatory Body (PSRB) links N/A	
Places of delivery Bournemouth University, Talbot Campus	
Mode(s) of delivery Full-time/Part-time	**Language of delivery** English
Typical duration Sept FT = 12 months Sept PT = 24 months Jan FT = 16 months Jan PT = 32 months	
Date of first intake September 2019	**Expected start dates** September January
Maximum student numbers N/A	**Placements** None
Partner(s) Not applicable	**Partnership model** Not applicable
Date of this Programme Specification January 2024	
Version number 1.4-0924	
Approval, review or modification reference numbers E20181916 BU 2021 01 - Approved 30/09/20, previously v1.0-0920 EC 2122 01- approved 23/09/2021 FST 2122 01 Approved 25/09/2021, previously version v1.1 0921 FST 2122 14 Approved 02/02/2022, previously version v1.2-0922 EC 2122 77 FST2324 15, approved 10/01/2024, previously v1.3	

Author
Dr. Michael Jones

PROGRAMME STRUCTURE

Programme Award and Title: MSc Cyber Security & Human Factors								
Stage 1/Level 7 Students are required to complete 4 core units and choose 2 optional units								
Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Cyber Security	Core	20		100%		30	2.0	100376
Human Factors	Core	20		100%		30	1.0	100736 (major), 100753 (minor)
Research Methods & Professional Issues	Core	20		100%		30	2.0	100962 (major), 101090 (minor)
Cyberpsychology	Core	20		100%		30	2.0	100993 (major), 100753 (minor)
Accessibility & Assistive Technologies	Option	20		100%		30	1.1	100736 (Major), 100958 (Minor), 100993 (Minor)
Blockchain & Digital Futures	Option	20		100%		30	1.0	100376 (Major), 100755 (Minor)
Security by Design	Option	20		100%		30	1.0	100736 (major); 100753 (minor)
Security Information and Event Management	Option	20		100%		30	1.0	100376 (major), 100755 (minor)
Progression requirements: There are no progression requirements. **Exit qualification:** PG Dip Cyber Security & Human Factors requires 120 credits at Level 7 (excluding 60 credit Individual Masters Project). PG Cert Computing requires 60 credits at Level 7.								

Stage 2/Level 7 Students are required to complete the Masters Project.								
Unit Name	**Core/ Option**	**No. of Credits**	**Assessment Element Weightings**			**Expected Contact hours per unit**	**Unit Version No.**	**HECoS Code** (plus balanced or major/minor load)
			Exam 1	**Cwk 1**	**Cwk 2**			
Individual Masters Project	Core	60		100%		10	1.0	100367 (Major), 100962 (Minor)
Exit qualification: MSc Cyber Security & Human Factors requires 180 credits at Level 7. PG Dip Cyber Security & Human Factors requires 120 credits at Level 7 (excluding 60 credit Individual Masters Project). PG Cert Computing requires 60 credits at Level 7.								

AIMS OF THE DOCUMENT

The aims of this document are to:

- define the structure of the programme;
- specify the programme award titles;
- identify programme and level learning outcomes;
- articulate the regulations governing the awards defined within the document.

AIMS OF THE PROGRAMME

Modern complex socio-technical systems need to reflect the business processes that they support. For many organisations their socio-technical infrastructure forms a core part of their business function. it is vital for individuals and teams developing and managing such systems to understand how the corporate strategy, business process, human-computer interfaces and cyber threat landscape shape the development of secure and effective socio-technical systems.

The MSc Cyber Security & Human Factors (CSHF) programme exposes graduates to all of these aspects of modern business systems. Instead of focussing on traditional Computer Sciences, greater emphasis is given to the development of architectures for effective interactive human-cyber systems. Graduates of the programme will have access to research and employment opportunities in the areas of cyber security, information assurance, and cyberpsychology.

The primary aim of this programme is the development of Masters level graduates who have

- a critical understanding of assurance methods, human factors and cyberpsychology practices and security management concepts required for supporting business process systems;
- a critical understanding in creating cutting-edge business risk analytics, interoperability of cross-domain solutions and originality in the application of knowledge and skills to create and manage security events;
- technical skills and competencies to work across data (clear, encrypted or transformed), secure information management, assured knowledge exchange, digital analytics, processes, technology and architecture of different industries and segments, such as defence, healthcare, hospitality, transportation and banking;
- research skills in areas such as literature reviews, critical analysis of research findings, project proposals, planning, experiment design and analysis, and dissemination.

ALIGNMENT WITH THE UNIVERSITY'S STRATEGIC PLAN

The MSc Cyber Security & Human Factors programme is informed by and well aligned with Bournemouth University's strategic plan and the fusion of excellent teaching, world-class research and professional practice that is at the heart of the institution's visions and values. Students are supported by academics with a wealth of industry experience, many of whom are actively engaged in various cyber security-related projects with several external organisations. Academics delivering the programme are actively engaged in cutting edge research, while students are encouraged to participate in a range of co-creation and co-publication projects. The programme's pedagogic approach offers students the opportunity to learn by engaging in a series of practical, industry focused tasks. These are aimed at equipping students with the full range of skills necessary to succeed in the contemporary cyber security environment, and are informed by the academic team's own industrial experience as well as by a network of industry contacts, who may also contribute directly to the programme by delivering guest lectures.

LEARNING HOURS AND ASSESSMENT

Bournemouth University taught programmes are composed of units of study, which are assigned a credit value indicating the amount of learning undertaken. The minimum credit value of a unit is normally 20 credits, above which credit values normally increase at 20-point intervals. 20 credits is the equivalent of 200 study hours required of the student, including lectures, seminars, assessment and independent study. 20 University credits are equivalent to 10 European Credit Transfer System (ECTS) credits.

The assessment workload for a unit should consider the total time devoted to study, including the assessment workload (i.e. formative and summative assessment) and the taught elements and independent study workload (i.e. lectures, seminars, preparatory work, practical activities, reading, critical reflection).

Assessment per 20 credit unit should normally consist of 3,000 words or equivalent. Dissertations and Level 6 and 7 Final Projects are distinct from other assessment types. The word count for these assignments is 5,000 words per 20 credits, recognizing that undertaking an in-depth piece of original research as the capstone to a degree is pedagogically sound.

STAFF DELIVERING THE PROGRAMME

Students will usually be taught by a combination of senior academic staff with others who have relevant expertise including – where appropriate according to the content of the unit – academic staff, qualified professional practitioners, demonstrators/technicians and research students.

PROGRAMME AND LEVEL 7 INTENDED PROGRAMME OUTCOMES

<table>
<tr><td>A: Knowledge and understanding

This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</td></tr>
<tr><td rowspan="2">A1 The cyber security development lifecycle: analysis, specification, design and implementation of socio-technical systems

A2 Critically appraising security risk and sustaining business continuity.

A3 Critically review the benefits of adopting Human Factors approaches in addressing socio-technical problems.

A4 Evaluate the alignment of information assurance architecture to a business process.

A5 Elucidate and evaluate the factors pertinent to Cyber Security and Cyberpsychology.

A6 Demonstrate critical understanding of methodology, research planning, and experiment design and analysis techniques.

A7 Acquire knowledge and understanding appropriate to subject area and the ability to handle inconsistency in the problem domain and produce a viable solution.</td><td>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):

• lectures (A1- A7);
• seminars (A1 – A7);
• workshops (A1 – A7);
• directed reading (A1 – A7);
• VLE (A1 – A7);
• independent research (for project) (A1 – A7).</td></tr>
<tr><td>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):

• examinations (A1 – A7);
• coursework (A1 – A7);
• project (A1 – A7).</td></tr>
</table>

<table>
<tr><td>B: Intellectual skills

This programme/level provides opportunities for students to:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</td></tr>
<tr><td rowspan="2">B1 Critical thinking, problem-solving and decision-making to solve complex security problems.

B2 Critical evaluation of cyber security processes, human factors and the relationships among them.

B3 Design of socio-technical systems to support secure business needs, synthesising processes, components and methods.

B4 Originality and creativity in applying cyber security and human factors knowledge to solve business systems problems.

B5 Professional judgement to balance risks, costs, benefits, reliability, assurance and protection.

B6 Critical evaluation of current research.

B7 Formulate, plan, execute and report on a project involving original design in a structured and disciplined manner.

B8 Communication of project outcomes to professional and academic standards.</td><td>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):

• lectures (B1- B8);

• seminars (B1 – B8);

• workshops (B1 – B8);

• VLE (B1 – B8);

• independent research (for project) (B1 – B8).</td></tr>
<tr><td>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):

• examinations (B1 – B8);

• coursework (B1 – B8);

• project (B1 – B8).</td></tr>
<tr><td>C: Practical skills

This programme/level provides opportunities for students to:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</td></tr>
<tr><td rowspan="2">C1 Establish the cyber security and human factors requirements of socio-technical systems with analysis of existing best practices and management of risk.

C2 Specify, design, model, implement and assess security architecture, patterns and systems.

C3 Conduct strategic and operational analysis, audit and management to formulate a security strategy, policies and governance.

C4 Determine, establish, test and maintain political, economic, socio-technical, environmental and legal factors to sustain an assured enterprise and applied methodologies.

C5 Manage or investigate information security incidents across systems.</td><td>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):

• lectures (C1 – C5);

• seminars and workshops (C1 – C5);

• VLE (C1 – C5);

• independent research (for project) (C1 – C5).</td></tr>
<tr><td>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):

• examinations (C1 – C5);
• coursework (C1 – C5);
• project (C1 – C4).</td></tr>
</table>

D: Transferable skills This programme/level provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:
D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas. **D2** Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media. **D3** Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere. **D4** Demonstrate initiative, self-direction and exercise personal responsibility for management of own learning. **D5** Work autonomously and become reflective learners. **D6** Communicate effectively and confidentially to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D6); • seminars (D1 – D6); • workshops (D1 – D6); • directed reading (D2 – D5); • VLE (D1 – D5); • independent research (for project) (D1 – D6). Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (D1 – D3); • coursework (D1 – D6); • project (D1 – D6).

The units of the Masters programme will run as lectures combined with seminars and/or practical sessions. The general assessment methodology consists of a variety of assessment options including writing research papers and/or technical reports; analysing real-world scenarios, and creating solutions to real-world or theoretical problems.

This Level 7 programme provides opportunities for students to develop and demonstrate knowledge, understanding, and skills.

Please refer to the course website for further information regarding admission regulations for this programme: MSc Cyber Security and Human Factors | Bournemouth University

PROGRESSION ROUTES

Recognition arrangements provide formally approved entry or progression routes through which students are eligible to apply for a place on a programme leading to a BU award. Recognition does not guarantee entry onto the BU receiving programme only eligibility to apply. In some cases, additional entry criteria such as a Merit classification from the feeder programme may also apply. Please see the Recognition Register (https://intranetsp.bournemouth.ac.uk/pandptest/7J_Recognition_Register_Public.xlsx) for a full list of approved Recognition arrangements and agreed entry criteria.

In order to take advantage of exciting new approaches to learning and teaching, as well as developments in industry, the current, approved Articulation/Recognition/Progression route(s) for this programme may be subject to change. Where this happens students will be informed and supported by the Faculty as early as possible.

ASSESSMENT REGULATIONS

The regulations for this programme are the University's Standard Postgraduate Assessment Regulations.

https://intranetsp.bournemouth.ac.uk/pandptest/6a-standard-assessment-regulations-postgraduate.pdf

Depending on practical considerations, it is intended that two assessment boards are held. One to follow the delivery of all non-project units, and the second one to consider the projects.

For MSc Cyber Security & Human Factors, students are eligible for the interim PGCert award upon completion of any 3 units (60 credits) and for PGDip award upon completion of all core units and 3 chosen optional units (120 credits).

WORK BASED LEARNING (WBL) AND PLACEMENT ELEMENTS

N/A

MSc Cyber Security & Human Factors Programme Skills Matrix

Stage	Unit	Programme Intended Learning Outcomes																									
		A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	B5	B6	B7	B8	C1	C2	C3	C4	C5	D1	D2	D3	D4	D5	D6

1	Cyber Security	X	X		X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
1	Human Factors		X	X		X	X	X	X	X	X	X		X		X	X		X	X		X	X	X	X	X	X
1	Research Methods & Professional Issues						X	X	X	X			X	X		X			X	X		X	X	X	X	X	X
1	Cyberpsychology	X		X		X	X	X	X	X	X	X		X		X	X		X	X		X	X	X	X	X	X
1	Blockchain and Digital Futures	X	X	X	X	X		X	X	X	X	X		X		X	X	X		X	X	X	X		X	X	X
1	Accessibility and Assistive Technologies	X		X	X	X	X	X	X	X			X	X		X		X	X	X	X	X		X	X	X	X
1	Security by Design	X		X		X	X	X	X		X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X
1	Security Information & Event Management	X	X			X	X	X	X			X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
2	Individual Masters Project	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

A – Subject Knowledge and Understanding

1. The cyber security development lifecycle: analysis, specification, design and implementation of socio-technical systems.
2. Critically appraising security risk and sustaining business continuity.
3. Critically review the benefits of adopting Human Factors approaches in addressing socio-technical problems.
4. Evaluate the alignment of information assurance architecture to a business process.
5. Elucidate and evaluate the factors pertinent to Cyber Security and Cyberpsychology.
6. Demonstrate critical understanding of methodology, research planning, and experiment design and analysis techniques.
7. Acquire knowledge and understanding appropriate to subject area and the ability to handle inconsistency in the problem domain and produce a viable solution.

B – Intellectual Skills

1. Critical thinking, problem solving and decision-making to solve complex security problems.
2. Critical evaluation of cyber security processes, human factors and the relationships among them.
3. Design of socio-technical systems to support secure business needs, synthesising processes, components and methods.
4. Originality and creativity in applying cyber security and human factors knowledge to solve business systems problems.
5. Professional judgement to balance risks, costs, benefits, reliability, assurance and protection.
6. Critical evaluation of current research.
7. Formulate, plan, execute and report on a project involving original design in a structured and disciplined manner.
8. Communication of project outcomes to professional and academic standards.

C – Subject Specific Skills

1. Establish the cyber security and human factors requirements of socio-technical systems with analysis of existing best practices and management of risk.
2. Specify, design, model, implement and assess security architecture, patterns and systems.
3. Conduct strategic and operational analysis, audit and management to formulate a security strategy, policies and governance.
4. Determine, establish, test and maintain political, economic, socio-technical, environmental and legal factors to sustain an assured enterprise and applied methodologies.
5. Manage or investigate information security incidents across systems.

D – Transferable Skills

1. Demonstrate problem solving skills and the application of knowledge across the discipline areas.
2. Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.
3. Distil, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.
4. Demonstrate initiative, self-direction and exercise personal responsibility for management of own learning.
5. Work autonomously and become reflective learners.
6. Communicate effectively and confidentially to appropriate professional and academic standards.