Programme Specification - Section 2

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 BSc (Hons) Cyber Security Management – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 / 120 (60 ECTS) Level 6 credits	
Intermediate award(s), title(s) and credits Dip HE Cyber Security – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 credits Cert HE Computing – 120 (60 ECTS) Level 4 credits	
UCAS Programme Code(s) (where applicable and if known) 2DA6	**HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load.** 100376, 100370
External reference points • The UK Quality Code for Higher Education; • Chapter A1: The National Level (incorporating the Framework for Higher Qualifications (FHEQ) in England, Wales and Northern Ireland); • Chapter A2: The Subject and Qualification Level (incorporating the Subject benchmark statements for Computing (2022)); • BCS – The Chartered Institute for IT guidelines • United Nations Sustainable Development Goals (SDGs) • The Cyber Security Body Of Knowledge www.cybok.org	
Professional, Statutory and Regulatory Body (PSRB) links BCS – The Chartered Institute for IT accreditation (https://www.bcs.org/media/1209/accreditation-guidelines.pdf)	
Places of delivery Bournemouth University, Talbot Campus	
Mode(s) of delivery Full-time / Full-time sandwich	**Language of delivery** English
Typical duration 3 years Full-time mode 4 years Sandwich mode	
Date of first intake September 2023	**Expected start dates** September 2023
Maximum student numbers N/A	**Placements** 30 weeks, optional
Partner(s) N/A	**Partnership model** N/A
Date of this Programme Specification July 2022	
Version number 2.0-0924	

Programme Specification - Section 2

Approval, review or modification reference numbers E2017063 FST 1718 10, approved 14/12/17 - previously v1.0-0918 BU 1819 01 FST 1920 21, approved 05/02/20 - previously v1.3-1219 BU 2021 01, approved 30/09/20 - previously v1.4-1220 FST 2122 10, approved 11/01/22 - previously v1.5-0921 Previously v1.6-0922 E212216 EC 2122 78 EC 2223 32
Author Dr Edward Apeh

PROGRAMME STRUCTURE

<table>
<tr><td colspan="9"><b>Programme Award and Title:</b> BSc (Hons) Cyber Security Management</td></tr>
<tr><td colspan="9"><b>Year 1/Level 4</b></td></tr>
<tr><td rowspan="2"><b>Unit Name</b></td><td rowspan="2"><b>Core/ Option</b></td><td rowspan="2"><b>No. of Credits</b></td><td colspan="3"><b>Assessment Element Weightings</b></td><td rowspan="2"><b>Expected Contact hours per unit</b></td><td rowspan="2"><b>Unit Version No.</b></td><td rowspan="2"><b>HECoS Code</b> (plus balanced or major/ minor load)</td></tr>
<tr><td><b>Exam 1</b></td><td><b>Cwk 1</b></td><td><b>Cwk 2</b></td></tr>
<tr><td>Computer Fundamentals</td><td>Core</td><td>20</td><td>50%</td><td>50%</td><td></td><td>36</td><td>3.0</td><td>100734
100735</td></tr>
<tr><td>Mathematics for Computing</td><td>Core</td><td>20</td><td>50%</td><td>50%</td><td></td><td>36</td><td>1.0</td><td>100400</td></tr>
<tr><td>Programming</td><td>Core</td><td>20</td><td>50%</td><td>50%</td><td></td><td>36</td><td>1.0</td><td>100956</td></tr>
<tr><td>Introduction to Cyber Security</td><td>Core</td><td>20</td><td></td><td>100%</td><td></td><td>36</td><td>1.0</td><td>100376</td></tr>
<tr><td>Network Essentials</td><td>Core</td><td>20</td><td></td><td>100%</td><td></td><td>36</td><td>1.0</td><td>100365</td></tr>
<tr><td>Computing and Society</td><td>Option</td><td>20</td><td></td><td>100%</td><td></td><td>36</td><td>1.0</td><td>100631
100367</td></tr>
<tr><td colspan="9"><b>Progression requirements:</b> Requires 120 credits at Level 4
<b>Exit qualification:</b> Cert HE Computing (requires 120 credits at Level 4)</td></tr>
</table>

Year 2/Level 5								
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**			
Information and Security Management	Core	20		100%		36	1.0	100370 100376
Security Operations (SecOps)	Core	20		100%		36	1.0	100376
Software Engineering	Core	20	30%	70%		36	2.0	100374
Network and Cyber Management	Core	20		100%		36	1.0	100365 100376
Technological Innovations in Cyber Security	Core	20	30%	70%		36	1.0	100360 100373
Software Business	Option	20		100%		36	1.0	100360

Progression requirements: Requires 120 credits at Level 5
Exit qualification: Dip HE Cyber Security (requires 120 credits at Level 4 and 120 credits at Level 5)

Optional placement year in industry/business:
Students who successfully complete the one-year placement will be awarded a degree in sandwich mode.

Progression requirements: Satisfactory completion of a minimum 30-week placement in industry/business and placement report.

Year 3/Level 6
Students are required to complete 2 core units, choose 1 optional unit and 1 open curriculum elective

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**			
Cybercrime	Core	20		100%		36	2.0	100376 100387
Human Computer Interaction	Core	20		100%		36	1.0	100736
Data Visualisation and Storytelling	Option	20		100%		36	1.0	100632 100755
Digital Innovation and Transformation	Option	20		100%		36	1.0	100362 101221
Systems Development	Option	20		100%		36	1.0	100374 100956
Digital Futures	Option	20		100%		36	1.0	100373 100440
Individual Project	Core	40		100%		21	1.0	100358 (major) 100812 (minor)

Exit qualification: BSc (Hons) Cyber Security Management; BSc Cyber Security Management

Sandwich UG award: Requires 120 credits at Level 4, 120 credits at Level 5, 120 credits at Level 6 and successful completion of a placement year.

Full-time UG award (with honours): Requires 120 credits at Level 4, 120 credits at Level 5 and 120 credits at Level 6

Full-time UG award (without honours): Requires 120 credits at Level 4, 120 credits at Level 5 and 80 credits at Level 6

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

This programme aims to produce high quality graduates who are skilled and knowledgeable in cyber security and its management, and to appeal to entrants interested in cyberspace and cyber security who come from a very broad spectrum of backgrounds.

This programme is distinctive because it develops the learner's interest in and understanding of the field of cyber security, including management of cyber security in a global context, the wider impacts of cyber security threat attack and defence on individual organisations and society, and complex socio-technical security problems.

In doing so, the programme aims to develop critically informed, agile and resourceful graduates, who:

- have the versatility and personal qualities to manage, implement and assess the security of business activities in a global context;
- have an understanding of the working of socio-technical systems in order to adequately prevent or respond to cyber security incidents;
- are critically aware of the wider impact of cyber security decisions on organisations (businesses, organisations) and society;
- have highly-developed interpersonal skills;
- are able to manage their own personal development and lifelong learning.

Graduates enter employment in a wide range of contexts and become lifelong learners with an appreciation of the value to society and the economy of an education in cyber, cyberspace, and the management of cyber security.

ALIGNMENT WITH THE UNIVERSITY'S STRATEGIC PLAN

The BSc (Hons) Cyber Security Management programme is informed by and well aligned with Bournemouth University's 2024 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. It promotes the digital & technological futures as well as the global security themes along with internal partnerships between faculties at Bournemouth University. Students are supported by academics with a wealth of industry experience, many of whom are actively engaged in various 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 innovative pedagogic approach offers students the opportunity to learn by engaging in a series of practical and 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. Staff, students and graduates will enrich society as active citizens in their communities. The programme is aligned with BU Strategic Plan for supporting the development of attributes such as global outlook and citizenship as well as contribute to society by having a significant impact on challenges worldwide through fusion.

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, recognising 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.

INTENDED LEARNING OUTCOMES – AND HOW THE PROGRAMME ENABLES STUDENTS TO ACHIEVE AND DEMONSTRATE THE INTENDED LEARNING OUTCOMES

PROGRAMME AND LEVEL 6 INTENDED PROGRAMME OUTCOMES

A: Subject knowledge and understanding This programme/level/stage provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
A1 Principles, techniques and concepts of cyber security management A2 Enabling technologies for cyber security management A3 A rigorous engineering approach to investigating and solving cyber security management problems in business context A4 The management and development of IT solutions to address cyber security and digital forensics or other problems	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1 – A5); • seminars (A1 – A5); • directed reading (A1 – A5); • use of the VLE (A1 – A5); • independent research (for dissertation) (A1 –A5).
A5 The professional, legal & ethical responsibilities of data science and AI personnel within the organisational, technical and global contexts in which cyber security and digital forensics are applied.	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • open book examinations (A1-A5); • coursework essays (A1 – A5); • dissertation (A1-A5).
B: Intellectual skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level outcomes:
B1 Critically thinking, problem-solving and decision-making to solve cyber security management problems; B2 Analyse, interpret, synthesise and critically evaluate information from current research; B3 Critically evaluate and justify alternative approaches to solutions development; B4 Formulate, plan, execute, and report on a cyber security management project involving original contributions; B5 Communicate findings to professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1 – B5); • seminars (B1 – B5); • directed reading (B1 –B5); • use of the VLE (B1 – B5); • independent research (for dissertation) (B1 – B5).

	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (B1- B5); • coursework essays (B1 – B5); • dissertation (B1 – B5).
C: Practical skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources; C2 Analyse, specify, design and implement cyber security management applications to meet business goals; C3 Select appropriate methods and tools for solving cyber security management problems; C4 Plan, monitor and evaluate the progress of a cyber security management solution.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1 – C4); • coursework essays (C1 – C4); • independent research for empirical dissertation (C1 – C4); • group exercises (C1 – C4).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (C1-C4); • coursework essays (C1-C4); • dissertation (C1- C4).
D: Transferable skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/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 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D4); • seminars (D1- D4); • use of the VLE (D1 – D4); • directed reading (D1- D4).

D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning. D5 Distill, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays (D1 – D4); • open book examinations (D1 – D4); • dissertation (D1- D4).

LEVEL 5/DipHE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level/stage provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
A1 Principles, techniques and concepts of cyber security management A2 Enabling technologies for cyber security management applications A4 The management and development of IT solutions to address cyber security management or other problems A5 The professional, legal & ethical responsibilities of data science and AI personnel within the organisational, technical and global contexts in which cyber security management is applied.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1, A2, A4, A5); • seminars (A1, A2, A4, A5); • directed reading (A1, A2, A4, A5); • use of the VLE (A1, A2, A4, A5).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (A1, A2, A4, A5); • coursework essays/presentations (A1, A2, A4, A5); • coursework design and implementation (A1, A2, A4, A5).
B: Intellectual skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
B1 Critically thinking, problem-solving and decision-making to solve cyber security management problems; B2 Analyse, interpret, synthesise and critically evaluate information from current research;	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1 – B3, B5);

B3 Critically evaluate and justify alternative approaches to solutions development; B5 Communicate findings to professional and academic standards.	• seminars (B1 – B3, B5); • directed reading (B1 – B3, B5) use of the VLE (B1 – B3, B5).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (B1 – B3, B5); • coursework essays/presentations (B1 – B3, B5). coursework design and implementation (B1 – B3, B5).
C: Practical skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources; C2 Analyse, specify, design and implement cyber security management applications to meet business goals; C3 Select appropriate methods and tools for solving cyber security management problems;	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1 – C3); • seminars (C1 – C3); group exercises (C1 – C3).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (C1-C3); • coursework design and implementation (C1 – C3).
D: Transferable skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage 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 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D1 – D4); • seminars (D1 – D4); • use of the VLE (D1 – D4); • group exercises (D1 – D4). • directed reading (D1 – D4).

D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (D1 – D4); • coursework essays/presentations (D1 – D4). • coursework design and implementation (D1 – D4).

LEVEL 4/Cert HE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level/stage provides opportunities for students to develop and demonstrate knowledge and understanding of*:*	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
Principles, techniques and concepts of cyber security management A4 The management and development of IT solutions to address cyber security management or other problems A5 The professional, legal & ethical responsibilities of cyber security and digital forensics within the organisational, technical and global contexts in which cyber security management is applied.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (A1, A4, A5); • seminars (A1, A4, A5); • directed reading (A1, A4, A5).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (A1, A4, A5); • coursework essays/presentations (A1, A4, A5). • coursework design and implementation (A1, A4, A5).
B: Intellectual skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
B1 Critically thinking, problem-solving and decision-making to solve cyber security management problems; B2 Analyse, interpret, synthesise and critically evaluate B5 Communicate findings to professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (B1, B2, B5); • seminars (B1, B2, B5); • directed reading (B1, B2, B5).

	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (B1, B2, B5); • coursework essays/presentations (B1, B2, B5). • coursework design and implementation (B1, B2, B5).
C: Practical skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
C1 Retrieve, select and evaluate information from a variety of sources; C3 Select appropriate methods and tools for solving cyber security management problems;	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (C1, C3); • seminars (C1, C3); • group exercises (C1, C3).
	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • examinations (C1, C3); • coursework essays/presentations (C1, C3). • coursework design and implementation (C1, C3).
D: Transferable skills This programme/level/stage provides opportunities for students to:	The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:
D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media. D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): • lectures (D2 – D4); • seminars (D2- D4); • use of the VLE (D2 – D4); • directed reading (D2- D4).

D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): • coursework essays/presentations (D2 – D4). • coursework design and implementation (D2 – D4). • examinations (D2 – D4).

Programme Skills Matrix

Units		Programme Intended Learning Outcomes																		
		A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	D1	D2	D3	D4	D5
LEVEL 6	Cybercrime	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Human Computer Interaction	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Systems Development	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Software Quality Assurance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Digital Innovation and Transformation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Data Visualisation & Storytelling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Individual Project	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Digital Futures (Elective)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
LEVEL 5	Information & Security Management	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
	Security Operations	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
	Software Engineering	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
	Technological Innovations in Cyber Security	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
	Network and Cyber Management	X	X		X	X	X	X	X		X	X	X	X		X	X	X	X	
	Software Business (Elective)	X	x		x	x	x	x	x		x	x	x	x		X	x	x	X	
LEVEL 4	Computer Fundamentals	X			X	X	X	X			X	X		X			X	X	X	
	Programming Fundamentals	X			X	X	X	X			X	X		X			X	X	X	
	Mathematics for Computing	X			X	X	X	X			X	X		X			X	X	X	
	Introduction to Cyber Security	X			X	X	X	X			X	X		X			X	X	X	
	Networks Fundamentals	X			X	X	X	X			X	X		X			X	X	X	
	Computing and Society (Elective)	X			x	x	x	x			x	x		X			x	x	X	

Programme Specification - Section 2

A – Subject Knowledge and Understanding This programme provides opportunities for students to develop and demonstrate knowledge and understanding of: 1. Principles, concepts and techniques of cyber security management; 2. Enabling technologies for cyber security management applications; 3. A rigorous engineering approach to investigating and solving cyber security management problems in business context; 4. The management and development of IT solutions to address cyber security management or other problems; 5. The professional, legal & ethical responsibilities of cyber security management personnel within the organisational, technical and global contexts in which cyber security manangement is applied.	**C – Subject-specific/Practical Skills** This programme provides opportunities for students to: 1. Retrieve, select and evaluate information from a variety of sources; 2. Analyse, specify, design and implement cyber security management applications to meet business goals; 3. Select appropriate methods and tools for solving cyber security management problems; 4. Plan, monitor and evaluate the progress of a cyber security management solution.
B – Intellectual Skills This programme provides opportunities for students to: 1. Critically thinking, problem-solving and decision-making to solve cyber security management problems; 2. Analyse, interpret, synthesise and critically evaluate information from current research; 3. Critically evaluate and justify alternative approaches to solutions development; 4. Formulate, plan, execute, and report on a cyber security management project involving original contributions; 5. Communicate findings to professional and academic standards.	**D – Transferable Skills** This programme provides opportunities for students to: 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. Structure and communicate ideas professionally and effectively to appropriate professional and academic standards. 4. Demonstrate initiative, self direction and exercise personal responsibility for management of own learning. 5. Distill, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.

ADMISSION REGULATIONS

Please refer to the course website for further information regarding admission regulations for this programme: BSc (Hons) Cyber Security Management | Bournemouth University

PROGRESSION ROUTES

Partnership arrangements provide formally approved progression routes through which students are eligible to apply for a place on a programme leading to a BU award. Please find information on Global Partnerships here: Global partnerships | Bournemouth University

ASSESSMENT REGULATIONS

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

WORK BASED LEARNING (WBL) AND PLACEMENT ELEMENTS

Students, under the guidance of lecturers and the Placement Office, are required to complete a sandwich year with a 30-week minimum placement requirement before level 6.

The placement is assessed on a pass/fail basis using the log book and employer appraisal. The 30-week sandwich placement must be completed between levels 5 and 6 and is a requirement for progression to level 6 for the successful completion of the sandwich mode award.

Placement draws on some or all of the units studied on the first two levels of the programme. It provides the opportunity for the student to develop their abilities and understanding of CSM and cyber-security related subjects, as well as providing a platform for successful entry into the profession following graduation. It applies and develops understanding and skills acquired in Levels 4 and 5 which makes a major contribution to the understanding of the final level units, and further develops final projects or dissertation research by utilising the context of the work experience as appropriate and enhances students' prospects of future employment.

Refer to *4K – Placements: Policy and Procedure* for more detail