

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 credits / 120 (60 ECTS) Level 6 credits Cert HE Computing – 120 (60 ECTS) Level 4 credits	
Intermediate award(s), title(s) and credits DipHE Cyber Security Management 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 credits CertHE Computing 120 (60 ECTS) Level 4	
UCAS Programme Code(s) (where applicable and if known) 2DA6	HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load. I990 (60%) Cyber Security 100366 (30%) Computer Science 100493 (10%) Applied Psychology
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 (2015)); - BCS – The Chartered Institute for IT guidelines	
Professional, Statutory and Regulatory Body (PSRB) links British Computer Society (BCS) accreditation (http://wam.bcs.org/wam/coursesearch.aspx#CoursesPL)	
Places of delivery Bournemouth University	
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 2019	Expected start dates September
Maximum student numbers Not applicable	Placements A minimum of 30 weeks
Partner(s) Not applicable	Partnership model Not applicable
Date of this Programme Specification September 2020	
Version number 1.5-0921	
Approval, review or modification reference numbers E2017063 FST 1718 10, approved 14/12/17. Previously version 1.0-0918 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	
Author Dr Edward Apeh	

Programme Specification – Section 1

PROGRAMME STRUCTURE

Programme Award and Title: BSc (Hons) Cyber Security Management									
Year 1/Level 4									
Students are required to complete all 6 core units									
Unit Name	Core/ Option	No of credits	Assessment Element Weightings			Expected contact hours per unit	Unit version no.	HESA HECoS code(s)	
			Exam 1	Cwk 1	Cwk 2			HECoS Subject Code and %	HECoS Subject Code and %
Principles of Programming	Core	20	50%	50%		48	1.1	100956 (100%)	
Computer Fundamentals	Core	20	50%	50%		48	2.1	100735 (50%)	100734 (50%)
Data and Databases	Core	20	50%	50%		48	3.1	100754 (50%)	100755 (50%)
Networks and Cyber Security	Core	20		50%	50%	48	1.1	100376 (50%)	100365 (50%)
Applications of Programming Principles	Core	20		100%		48	1.1	100956 (70%)	100373 (30%)
Business Systems Analysis and Design	Core	20	30%	70%		48	2.1	100753 (50%)	100360 (50%)
Progression requirements: Requires 120 credits at Level 4									
Exit qualification: Cert HE Computing (requires 120 credits at Level 4)									

Programme Specification – Section 1

Year 2/Level 5									
Students are required to complete all 6 core units									
Unit Name	Core/ Option	No of credits	Assessment Element Weightings			Expected contact hours per unit	Unit version no.	HESA HECoS code(s)	
			Exam 1	Cwk 1	Cwk 2			HECoS Subject Code and %	HECoS Subject Code and %
Digital Forensics Fundamentals	Core	20		100%		36	3.1	100385 (100%)	
Cyber Security Management	Core	20	50%	50%		36	2.1	100376 (50%)	101040 (50%)
Enterprise Security and Privacy	Core	20	50%	50%		36	2.1	100373 (50%)	100376 (50%)
Economics of Information Security	Core	20		100%		36	2.2	100376 (100%)	
Security Information and Event Management	Core	20		100%		36	2.1	100823 (70%)	100812 (30%)
Cyber Psychology	Core	20		40%	60%	36	2.1	100493 (100%)	
Progression requirements: Requires 120 credits at Level 5 Exit qualification: Dip HE Cyber Security Management (requires 120 credits at Level 4 and 120 credits at Level 5)									
Year 3/Level P - Compulsory placement year in industry/business For programmes with a compulsory placement - exemption is possible for those who have worked in industry/business at a relevant level Progression requirements: Satisfactory completion of a minimum 30-week placement in industry/business and placement report.									

Programme Specification – Section 1

Year 3/4/Level 6									
Students are required to complete 3 core units and choose 1 optional units									
Unit Name	Core/ Option	No of credits	Assessment Element Weightings			Expected contact hours per unit	Unit version no.	HESA HECoS code(s)	
			Exam 1	Cwk 1	Cwk 2			HECoS Subject Code and %	HECoS Subject Code and %
Advanced Digital Forensics	Option	20		100%		36	1.1	100385 (100%)	
Business Continuity Management*	Option	20		100%		36	2.2	100823 (100%)	
Cybercrime	Core	20		100%		36	1.1	100482 (40%)	100376 (60%)
Cyber Situational Awareness	Core	20		100%		36	3.1	100359 (50%)	100992 (50%)
Human Factors in Computing Systems	Option	20		100%		36	3.1	100736 (100%)	
Information Assurance*	Option	20		100%		36	3.1	100376 (100%)	
Individual Project	Core	60		100%		21	3.1	100358 (60%)	100812 (40%)

* = may not run, depends on student numbers and staff availability.

Exit qualification: BSc (Hons) 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: Requires 120 credits at Level 4, 120 credits at Level 5 and 120 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 2012-18 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 global security theme and 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.

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.

Programme Specification - Section 2

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

<p>A: Subject knowledge and understanding</p> <p>This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:</p>
<p>A1 Information assurance and cyber security management</p> <p>A2 Cyber situational awareness, governance, risk and controls in an organisational context</p> <p>A3 A specialist subject of the student's choice in an area offered by the Programme at Level 6</p> <p>A4 The development of software or other IT solutions to cyber security problems</p> <p>A5 Psychological, legal, and socio-technical context of cybercrime</p> <p>A6 The professional, legal & ethical responsibilities of security personnel within the organisational, technical and global contexts in which cyber security is applied</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (A1 – A6); • seminars (A1 – A6); • directed reading (A1 – A6); • use of the VLE (A1 – A6); • independent research (for dissertation) (A1 – A6).
<p>B: Intellectual skills</p> <p>his programme/level provides opportunities for students to:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level outcomes:</p>
	<p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (A1-A3, A5-A6); • coursework essays (A1-A3, A5-A6); • dissertation (A1 – A6).

Programme Specification - Section 2

<p>B1 Reason critically</p> <p>B2 Exercise independence of thought</p> <p>B3 Analyse, interpret, evaluate and synthesise</p> <p>B4 Identify and solve problems</p> <p>B5 Select and apply appropriate management methods to the solution of problems</p> <p>B6 Evaluate resource requirements of alternative solutions</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (B1 - B4); • seminars (B1 – B6); • directed reading (B1 – B6); • use of the VLE (B2 – B6); • independent research (for dissertation) (B1 – B6). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (B1- B5); • coursework essays (B1 – B6); • dissertation (B1 – B6).
<p>C: Practical skills</p> <p>This programme/level provides opportunities for students to:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:</p>
<p>C1 Retrieve, select and evaluate information from a variety of sources</p> <p>C2 Formulate a set of requirements for an assured solution</p> <p>C3 Analyse a cyber-security problem</p> <p>C4 Plan the implementation of a cyber-security problem solution</p> <p>C5 Evaluate an assured socio-technical system</p> <p>C6 Plan, monitor and evaluate the progress of a cyber-security or cyber security-related project.</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (C1 – C5); • coursework essays (C1 – C5); • independent research for empirical dissertation (C1 – C6); • group exercises (C3 – C5). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (C2 – C5); • coursework essays (C1 – C5); • dissertation (C1 – C6).
<p>D: Transferable skills</p> <p>This programme/level provides opportunities for students to:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the programme/level learning outcomes:</p>

Programme Specification - Section 2

D1	Structure and communicate ideas effectively both orally and in writing	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> • lectures (D1 - D5); • seminars (D1- D5); • use of the VLE (D1 - D5); • directed reading (D1- D5).
D2	Learn independently in complicated contexts	
D3	Work professionally as an individual to develop creative solutions to problems	
D4	Work professionally in teams to develop creative solutions to problems	
D5	Deploy a range of interpersonal skills including effective listening, negotiating, persuasion and presentation	
		Assessment strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> • coursework essays (D1 - D5); • examinations (D1 - D5); • dissertation (D1- D5).

LEVEL 5/DipHE INTENDED LEVEL OUTCOMES

A: Knowledge and understanding This programme/level 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 learning outcomes:
A1	Cyber security management principles and techniques of assessing the security of the different platforms on which socio-technical systems operate	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> • lectures (A1- A6); • seminars (A1 – A6); • directed reading (A1, A3); • use of the VLE (A1 – A6); • independent research (A1 – A6).
A2	The principles and techniques of computer forensic science and digital security.	
A3	The principles and techniques of project management and of working professionally and ethically in teams	
A4	Cyber psychology, online behaviour and the Insider Threat	
A5	Cyber security solution cost benefit analysis and the financial motivation for initiating, developing and using assured socio-technical systems	
A6	The common operational cyber security picture	
		Assessment strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> • examinations (A1, A4 –A5); • coursework essays/presentations (A1 – A6); • group exercises (A1, A3, A5 – A6).

Programme Specification - Section 2

B: Intellectual skills		The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:
This programme/level provides opportunities for students to:		
B1	Apply appropriate analysis, design and development concepts to problems of intermediate complexity, with minimal guidance	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):
B2	Analyse processes and problems, and specify, design and evaluate appropriate solutions	
B3	Investigate technologies and approaches systematically and show how they can be used to solve problems	
B4	Understand the factors that affect how people work in teams	Assessment strategies and methods (referring to numbered Intended Learning Outcomes):
C: Practical skills		The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:
This programme/level provides opportunities for students to:		
C1	Analyse and develop a cyber-security program of intermediate complexity	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):
C2	Select appropriate platforms and security measures for different socio-technical systems	
C3	Analyse the psychological concepts relevant to human use of and interaction with computer technology	
C4	Work in teams to manage and monitor cyber security projects of intermediate size and complexity	
C5	Forensically capture and analyse data held on digital devices	
C6	Evaluate the economic costs and financial implications of information security strategy	Assessment strategies and methods (referring to numbered Intended Learning Outcomes):
D: Transferable skills		The following learning and teaching and assessment strategies and methods

Programme Specification - Section 2

<p>This programme/level provides opportunities for students to:</p>	<p>enable students to achieve and to demonstrate the level learning outcomes:</p>
<p>D1 Organise and use ideas to communicate orally and in writing</p> <p>D2 Learn independently in contexts of intermediate complexity</p> <p>D3 Work as an individual to seek solutions to problems, with minimal guidance</p> <p>D4 Work ethically and professionally in teams to seek solutions to problems, with minimal guidance</p> <p>D5 Plan the monitoring activity of a cyber-security project of Intermediate size and complexity</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (D1 - D5); • seminars (D1- D5); • use of the VLE (D1 - D5); • directed reading (D1- D5). • Active/PB Learning approaches <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • coursework essays (D1 - D5); • coursework design and implementation (D1 - D5);

LEVEL 4/Cert HE INTENDED LEVEL OUTCOMES

<p>A: Knowledge and understanding</p> <p>This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</p>
<p>A1 Basic principles of programming using one of the major programming languages</p> <p>A2 Principles and techniques of database design and development</p> <p>A3 Principles and techniques of systems analysis and design in a commercial context</p> <p>A4 Principles of computer networks and security</p> <p>A5 The principles and techniques of designing and developing usable applications</p> <p>A6 Principles of computers and operating systems</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (A1- A4); • seminars (A1 – A4); • directed reading (A1, A3); • use of the VLE (A4, A5); <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (A1 – A6); • coursework essays (A2 – A5);

Programme Specification - Section 2

	<ul style="list-style-type: none"> coursework design and implementation (A1, A2, A4, A6)
<p>B: Intellectual skills</p> <p>This programme/level provides opportunities for students to:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</p>
<p>B1 Apply analysis, design and development concepts with guidance, using given principles</p> <p>B2 Analyse small well-defined scenarios and design, and implement and test appropriate solutions</p> <p>B3 Analyse, categorise and interpret data and information</p> <p>B4 Utilise analyses to plan and develop further investigations</p> <p>B5 Identify and investigate computing security issue.</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> lectures (B1 – B5); seminars (B1 – B5); directed reading (B1 – B5); use of the VLE (B1 – B5); <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> examinations (B1- B4); coursework essays (B1 - B5); coursework design and implementation (B1, B2, B5)
<p>C: Practical skills</p> <p>This programme/level provides opportunities for students to:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</p>
<p>C1 Write computer programs to solve simple problems</p> <p>C2 Design and implement databases using a query language</p> <p>C3 Set up and configure a simple system (a computer or small network) with consideration of cyber security</p> <p>C4 Design and build simple applications applying design principles</p> <p>C5 Use and apply modelling techniques to analyse and design solutions to simple problems representative for a commercial context</p> <p>C6 Work in small teams to solve simple development problems</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> lectures (C1 – C6); coursework essays (C1 – C6); group exercises (C4, C5). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> coursework design and implementation (C1 – C6); reflection (C1 – C6).

Programme Specification - Section 2

<p>D: Transferable skills</p> <p>This programme/level provides opportunities for students to:</p>	<p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</p>
<p>D1 Communicate orally and in writing using appropriate structures, facts and events</p> <p>D2 Conduct and report within a set time and context on work assigned</p> <p>D3 Find facts to describe and explain simple phenomena and artefacts</p> <p>D4 Work independently to achieve set goals</p> <p>D5 Work efficiently and effectively in small groups within limited and set contexts</p> <p>D6 Appreciate the professional and ethical issues involved in IT.</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (D1 – D6); • seminars (D1 – D6); • use of the VLE (D1 – D6); • directed reading (D1 – D6). <hr/> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • coursework essays (D1 – D6); • examinations (D1 – D6); • presentations (D1 – D6).

ADMISSION REGULATIONS

The regulations for this programme are the University's Standard Undergraduate/Postgraduate/Graduate Diploma/Graduate Certificate Admission Regulations with the following exceptions:

The regulations for this programme are the University's Standard Undergraduate Admission Regulations with the following exceptions: Applicants whose mother tongue is not English must offer evidence of qualifications in written and spoken English. Acceptable qualifications are: IELTS (academic) 6.5 (with a minimum of 6 in each of four categories) or direct equivalent.

<https://intranetsp.bournemouth.ac.uk/pandptest/3a-undergraduate-admissions-regulations.doc>.

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 Undergraduate Assessment Regulations.

[https://intranetsp.bournemouth.ac.uk/pandptest/6a-standard-assessment-regulations-undergraduate%20\(2\).docx](https://intranetsp.bournemouth.ac.uk/pandptest/6a-standard-assessment-regulations-undergraduate%20(2).docx)

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 40 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 details.

Programme Skills Matrix

Units		Programme Intended Learning Outcomes																						
		A 1	A 2	A 3	A 4	A 5	A 6	B 1	B 2	B 3	B 4	B 5	B 6	C 1	C 2	C 3	C 4	C 5	C 6	D 1	D 2	D 3	D 4	
L	Advanced Digital Forensics	X		X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
E	Business Continuity Management	X		X			X	X	X	X	X	X		X	X	X		X			X		X	
V	Cybercrime	X	X			X	X	X	X	X	X			X	X			X			X	X	X	
E	Cyber Situational Awareness	X	X		X		X	X	X	X	X	X	X	X	X			X			X	X	X	
L	Human Factors in Comp. Systems	X		X			X	X	X	X	X	X	X	X	X			X			X	X	X	
6	Information Assurance	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	X	X	
L	Digital Forensics Fundamentals	X			X		X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	
E	Cyber Security Management	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	
V	Cyber Psychology	X	X			X		X	X	X				X							X		X	
E	Economics of Information Security	X	X		X		X	X	X	X	X			X							X	X	X	X
L	Enterprise Security and Privacy	X	X		X		X	X	X	X	X			X	X	X		X			X	X	X	
5	Security Information and Event Management	X	X		X		X	X	X	X	X		X	X	X	X		X			X	X	X	X
L	Principles of Programming				X			X	X	X	X	X		X		X	X				X	X	X	
E	Computer Fundamentals	X			X			X	X	X	X			X	X		X	X			X	X	X	
V	Data & Databases	X			X		X	X	X	X	X			X				X			X	X	X	
E	Networks and Cyber Security	X	X		X	X	X	X	X	X	X	X		X	X	X		X			X	X	X	
L	Applications of Programming Principles				X			X	X	X	X	X		X		X	X				X	X	X	
4	Business Systems Analysis & Design				X		X	X	X	X	X	X		X	X	X					X	X	X	X
A – Subject Knowledge and Understanding This programme provides opportunities for students to develop and demonstrate knowledge and understanding of: <ol style="list-style-type: none"> Information assurance and cyber security management Cyber situational awareness, governance, risk and controls in an organisational context A specialist subject of the student's choice in an area offered by the Programme at Level 6 The development of software or other IT solutions to cyber security problems Psychological, legal, and socio-technical context of cybercrime The professional, legal & ethical responsibilities of security personnel within the organisational, technical and global contexts in which information security is applied 								C – Subject-specific/Practical Skills This programme provides opportunities for students to: <ol style="list-style-type: none"> Retrieve, select and evaluate information from a variety of sources Formulate a set of requirements for an assured solution Analyse a cyber-security problem Plan the implementation of a cyber-security problem solution Evaluate an assured socio-technical system Plan, monitor and evaluate the progress of a cyber-security or cyber security-related project. 																
B – Intellectual Skills This programme provides opportunities for students to: <ol style="list-style-type: none"> Reason critically Exercise independence of thought Analyse, interpret, evaluate and synthesise Identify and solve problems Select and apply appropriate management methods to the solution of problems Evaluate resource requirements of alternative solutions 								D – Transferable Skills This programme provides opportunities for students to: <ol style="list-style-type: none"> Structure and communicate ideas effectively both orally and in writing Learn independently in complicated contexts Work professionally as an individual to develop creative solutions to problems Work professionally in teams to develop creative solutions to problems 																