

## KEY PROGRAMME INFORMATION

<b>Originating institution(s)</b> Bournemouth University	<b>Faculty responsible for the programme</b> Faculty of Science and Technology
<b>Final award(s), title(s) and credits</b> BSc (Hons) Forensic Computing & Security – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 / 120 (60 ECTS) Level 6 credits	
<b>Intermediate award(s), title(s) and credits</b> Dip HE Forensic Computing & Security – 120 (60 ECTS) Level 4 / 120 (60 ECTS) Level 5 credits Cert HE Computing – 120 (60 ECTS) Level 4 credits	
<b>UCAS Programme Code(s) (where applicable and if known)</b> G550	<b>HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load.</b> 100366 (30%) Computer science 1990 (70%) Forensic Computing and Security
<b>External reference points</b> - 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	
<b>Professional, Statutory and Regulatory Body (PSRB) links</b> BCS – The Chartered Institute for IT accreditation ( <a href="http://wam.bcs.org/wam/coursesearch.aspx#CoursesPL">http://wam.bcs.org/wam/coursesearch.aspx#CoursesPL</a> )	
<b>Places of delivery</b> Bournemouth University	
<b>Mode(s) of delivery</b> Full-time sandwich (Full-time without placement)	<b>Language of delivery</b> English
<b>Typical duration</b> 4 years (3 years without placement)	
<b>Date of first intake</b> September 2019	<b>Expected start dates</b> September
<b>Maximum student numbers</b> Not applicable.	<b>Placements</b> A minimum of 30 weeks
<b>Partner(s)</b> Not applicable	<b>Partnership model</b> Not applicable
<b>Date of this Programme Specification</b> November 2021	
<b>Version number</b> 1.5-0923	
<b>Approval, review or modification reference numbers</b> E2017036 FST 1718 10, approved 14/12/17, previously v1.0-0918 BU 1819 01 FST 1920 21, approved 05/02/20 -previously v1.2-0919 BU 2021 01, approved 30/09/20 - previously v1.3-0920 FST 2122 10, approved 11/01/22 - previously v1.4-0922 EC 2122 78 EC 2223 02	

## Programme Specification – Section 1

EC 2223 32
<b>Author</b> Dr Alexios Mylonas

## Programme Specification – Section 1

### PROGRAMME STRUCTURE

<b>Programme Award and Title:</b> BSc (Hons) Forensic Computing & Security									
<b>Year 1/Level 4</b> 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			HESA HECoS Subject Code and %	HESA HECoS Subject Code and %
Principles of Programming	Core	20	50%	50%		48	1.1	100956 (100%)	
Computer Fundamentals	Core	20	50%	50%		48	2.2	100735 (50%)	100734 (50%)
Data and Databases	Core	20	50%	50%		48	4.2	100754 (50%)	100755 (50%)
Networks and Cyber Security	Core	20	50%	50%		48	2.2	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%)
<b>Progression requirements:</b> Requires 120 credits at Level 4									
<b>Exit qualification:</b> Cert HE Computing (requires 120 credits at Level 4)									

## Programme Specification – Section 1

<b>Year 2/Level 5</b> 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			HESA HECoS Subject Code and %	HESA HECoS Subject Code and %
Digital Forensics Fundamentals	Core	20		100%		36	3.1	100385 (100%)	
Ethical Hacking & Countermeasures	Core	20	50%	50%		36	3.1	100376 (100%)	
Enterprise Security and Privacy	Core	20	50%	50%		36	2.1	100373 (50%)	100376 (50%)
Project Management & Teamwork	Core	20		100%		24	4.1	100812 (100%)	
Tools and Technologies of Data Science	Core	20	30%	70%		36	1.1	100367 (50%)	100741 (50%)
Security Information and Event Management	Core	20		100%		36	2.1	100823 (70%)	100812 (30%)
<b>Progression requirements:</b> Requires 120 credits at Level 5									
<b>Exit qualification:</b> Dip HE Forensic Computing & Security (requires 120 credits at Level 4 and 120 credits at Level 5)									
<b>Year 3/Level P - Compulsory placement year in industry/business</b>									
For programmes with a compulsory placement - exemption is possible for those who have worked in industry/business at a relevant level.									
<b>Progression requirements:</b> Satisfactory completion of a minimum 30-week placement in industry/business and placement report.									

## Programme Specification – Section 1

<b>Year 3/4/Level 6</b>									
Students are required to complete all core units and one option unit									
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			HESA HECoS Subject Code and %	HESA HECoS Subject Code and %
Advanced Digital Forensics	Core	20		100%		36	1.1	100385 (100%)	
Business Continuity Management	Option	20		100%		36	2.2	100823 (100%)	
Cybercrime	Option	20		100%		36	1.1	100482 (40%)	100376 (60%)
Cyber Situational Awareness	Option	20		100%		36	3.1	100359 (50%)	100992 (50%)
Information Assurance*	Option	20		100%		36	3.1	100376 (100%)	
Machine Intelligence*	Option	20		100%		36	3.1	100359 (50%)	100992 (50%)
Security by Design	Core	20	50%	50%		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) Forensic Computing & Security  
**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

BSc (Hons) Forensic Computing & Security is offered to provide for those particularly interested in a career involving computer forensics and/or computer security. It is based on the premise that computer forensics and computer security is an expanding field, covering not only computers but other computing systems such as mobile devices, satellite navigation systems, and Internet of Things (IoT) devices. The programme equips graduates the skills and knowledge that is necessary to excel in the security and/or forensics industry.

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 the ability to weaponise technology to prevent or respond to security incidents
- are critically aware of the wider impact of security decisions on organisations (businesses, organisations) and society;
- have highly-developed interpersonal skills;
- are able to manage their own personal development and lifelong learning.

### ALIGNMENT WITH THE UNIVERSITY'S STRATEGIC PLAN

The BSc (Hons) Forensic Computing & Security programme is informed by and 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. Students are supported by academics with considerable experience in the security industry. 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, industry focused tasks. These are aimed at equipping students with the full range of skills necessary to succeed cyber security arena.

### 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

<p><b>A: Subject knowledge and understanding</b></p> <p>This programme 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 learning outcomes:</p>
<p>A1 Information assurance and security, A2 Digital forensic science and governance, A3 A specialist subject of the student's choice in an area offered by the Programme at Level 6, A4 How forensic and ethical hacking processes can be used to support information security, A5 The development of software or other IT solutions to address security and digital forensics related problems, A6 The professional, legal &amp; ethical responsibilities of security personnel within the organisational, technical and global contexts in which information security is applied.</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (A1 – A6);</li> <li>• seminars (A1 – A6);</li> <li>• directed reading (A1 – A6);</li> <li>• use of the VLE (A1 – A6);</li> <li>• independent research (for dissertation) (A1 –A6).</li> </ul> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (A1-A4, A6);</li> <li>• coursework essays (A1-A4, A6);</li> <li>• dissertation (A1 – A6).</li> </ul>
<p><b>B: Intellectual skills</b></p> <p>This programme 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 outcomes:</p>
<p>B1 Reason critically, B2 Demonstrate independent thought, B3 Analyse, interpret, synthesise and evaluate information, B4 Identify and solve problems, B5 Select and apply appropriate design methods to the solution of problems, 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"> <li>• lectures (B1 - B4);</li> <li>• seminars (B1 – B6);</li> <li>• directed reading (B5 – B6);</li> <li>• use of the VLE (B2 – B5);</li> </ul>

## Programme Specification - Section 2

	<ul style="list-style-type: none"> <li>• independent research (for dissertation) (B1 – B6).</li> </ul> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (B1- B5);</li> <li>• coursework essays (B1 – B6);</li> <li>• dissertation (B1 – B6).</li> </ul>
<p><b>C: Practical skills</b></p> <p>This programme 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 learning outcomes:</p>
<p>C1 Retrieve, select and evaluate information from a variety of sources,</p> <p>C2 Formulate a set of requirements for a security and/or digital forensics solution,</p> <p>C3 Design a solution to a security and/or digital forensics related problem,</p> <p>C4 Implement a solution to a security and/or digital forensics related problem,</p> <p>C5 Evaluate a system or software with regards to security and/or digital forensics,</p> <p>C6 Plan, monitor and evaluate the progress of a security and/or digital forensics related project.</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (C1 – C6);</li> <li>• coursework essays (C1 - C3, C5);</li> <li>• independent research (C1 – C6);</li> <li>• group exercises (C1 – C6).</li> </ul> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (C2, C5);</li> <li>• coursework (C1 –C5);</li> <li>• dissertation (C1 –C6).</li> </ul>
<p><b>D: Transferable skills</b></p> <p>This programme 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 learning outcomes:</p>
<p>D1 Structure and communicate ideas effectively both orally and in writing;</p> <p>D2 Learn independently in complicated contexts;</p> <p>D3 Work professionally as an individual to develop creative solutions to problems;</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (D1 – D4);</li> <li>• seminars (D1- D4);</li> <li>• use of the VLE (D1 – D4);</li> </ul>



## Programme Specification - Section 2

D4 Work professionally in teams to develop creative solutions to problems.	<ul style="list-style-type: none"> <li>• directed reading (D1- D4).</li> </ul>
	<p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• coursework essays (D1 – D4);</li> <li>• open book examinations (D1 – D4);</li> <li>• dissertation (D1- D4).</li> </ul>

### LEVEL 5/Dip HE INTENDED LEVEL OUTCOMES

<p><b>A: Knowledge and understanding</b></p> <p>This 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 The principles and techniques of assessing the security of the different platforms on which IT systems</p> <p>A2 The principles and techniques of computer forensic science and digital security.</p> <p>A3 The principles and techniques of project management and of working professionally and ethically in teams,</p> <p>A4 The principles and techniques of artificial intelligence</p> <p>A5 The principles and technique of identifying attacks from machine data</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (A1- A5);</li> <li>• seminars (A1 – A5);</li> <li>• directed reading (A1, A3);</li> <li>• use of the VLE (A1 - A5);</li> <li>• independent research (A1 –A5).</li> </ul>
	<p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (A1 – A4);</li> <li>• coursework essays (A1 – A5);</li> </ul>
<p><b>B: Intellectual skills</b></p> <p>This 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 appropriate analysis, design and development concepts to problems of intermediate complexity, with minimal guidance,</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (B1 - B4);</li> </ul>

## Programme Specification - Section 2

<p>B2 Analyse processes and problems, and specify, design and evaluate appropriate solutions,</p> <p>B3 Investigate technologies and approaches systematically and show how they can be used to solve problems,</p> <p>B4 Understand the factors that affect how people work in teams.</p>	<ul style="list-style-type: none"> <li>• seminars (B1 – B4);</li> <li>• directed reading (B1 – B4);</li> <li>• use of the VLE (B1 – B4).</li> <li>• independent research (B1 – B4).</li> </ul> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (B1- B4);</li> <li>• coursework essays (B1 – B4).</li> <li>• group exercises (B4).</li> </ul>
<p><b>C: Practical skills</b></p> <p>This 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 Plan and conduct a simple penetration test,</p> <p>C2 Select appropriate platforms and security measures for different IT systems,</p> <p>C3 Specify, design and evaluate IT solutions to security problems of intermediate complexity,</p> <p>C4 Work in teams to manage and monitor forensic investigation projects of intermediate size and complexity</p> <p>C5 Forensically capture and analyse data held on digital devices,</p> <p>C6 Analyse machine data to identify or prevent security incidents.</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (C1 - C3);</li> <li>• seminars (C1 – C5);</li> <li>• group exercises (C4 – C6).</li> </ul> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (C1, C3, C5);</li> <li>• coursework essays (C1 –C6).</li> </ul>
<p><b>D: Transferable skills</b></p> <p>This 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 Organise and use ideas to communicate orally and in writing,</p> <p>D2 Learn independently in contexts of intermediate complexity,</p>	<p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (D1 – D4);</li> <li>• seminars (D1- D4);</li> </ul>

## Programme Specification - Section 2

<p>D3 Work as an individual to seek solutions to problems, with minimal guidance,</p> <p>D4 Work ethically in teams to seek solutions to problems, with minimal guidance.</p>	<ul style="list-style-type: none"> <li>• use of the VLE (D1 – D4);</li> <li>• directed reading (D1- D4).</li> </ul>
	<p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• coursework essays (D1 – D4);</li> <li>• examinations (D1 – D4).</li> </ul>

### LEVEL 4/Cert HE INTENDED LEVEL OUTCOMES

<p><b>A: Knowledge and understanding</b></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"> <li>• lectures (A1- A4);</li> <li>• seminars (A1 – A4);</li> <li>• directed reading (A1, A3);</li> <li>• use of the VLE (A4, A5);</li> </ul> <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• examinations (A1 – A6);</li> <li>• coursework essays (A2 – A5);</li> <li>• coursework design and implementation (A1, A2, A4, A6)</li> </ul>
<p><b>B: Intellectual skills</b></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>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> <li>• lectures (B1 – B5);</li> <li>• seminars (B1 – B5);</li> </ul>

## Programme Specification - Section 2

B3	Analyse, categorise and interpret data and information	<ul style="list-style-type: none"> <li>• directed reading (B1 – B5);</li> <li>• use of the VLE (B1 – B5);</li> </ul>
B4	Utilise analyses to plan and develop further investigations	
B5	Identify and investigate computing security issue.	
<b>C: Practical skills</b> 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:
C1	Write computer programs to solve simple problems	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> <li>• lectures (C1 – C6);</li> <li>• coursework essays (C1 – C6);</li> <li>• group exercises (C4, C5).</li> </ul>
C2	Design and implement databases using a query language	
C3	Set up and configure a simple system (a computer or small network) with consideration of cyber security	
C4	Design and build simple applications applying design principles	Assessment strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> <li>• coursework design and implementation (C1 – C6);</li> <li>• reflection (C1 – C6).</li> </ul>
C5	Use and apply modelling techniques to analyse and design solutions to simple problems representative for a commercial context	
C6	Work in small teams to solve simple development problems	
<b>D: Transferable skills</b> 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	Communicate orally and in writing using appropriate structures, facts and events	Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes): <ul style="list-style-type: none"> <li>• lectures (D1 – D6);</li> <li>• seminars (D1 – D6);</li> <li>• use of the VLE (D1 – D6);</li> </ul>
D2	Conduct and report within a set time and context on work assigned	
D3	Find facts to describe and explain simple phenomena and artefacts	

## Programme Specification - Section 2

D4 Work independently to achieve set goals	<ul style="list-style-type: none"><li>• directed reading (D1 – D6).</li></ul>
D5 Work efficiently and effectively in small groups within limited and set contexts	Assessment strategies and methods (referring to numbered Intended Learning Outcomes):
D6 Appreciate the professional and ethical issues involved in IT.	

## ADMISSION REGULATIONS

Please refer to the course website for further information regarding admission regulations for this programme: [BSc \(Hons\) Forensic Computing and Security | 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 BIT and 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, makes a major contribution to the understanding of the final level units, 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	
E	Business Continuity Management	X		X			X	X	X	X	X	X		X	X	X		X		X		X	
V	Cyber Crime,	X	X	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	X
L	Information Assurance	X	X		X			X	X	X	X	X	X	X	X	X		X		X	X	X	
6	Machine Intelligence			X				X	X	X	X	X	X	X	X					X	X	X	
	Security by Design	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	
L	Digital Forensics Fundamentals		X		X		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	
E	Ethical Hacking & Countermeasures	X			X		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	
V	Enterprise Security and Privacy	X	X				X	X	X	X	X	X		X	X	X		X		X	X	X	
E	Project Management & Teamwork	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
L	Tools & Technologies of Data Science		X			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	
4	Business Systems Analysis and Design					X	X	X	X	X	X	X	X	X	X	X				X	X	X	X
<b>A – Subject Knowledge and Understanding</b> This programme provides opportunities for students to develop and demonstrate knowledge and understanding of: <ol style="list-style-type: none"> <li>Information assurance and security.</li> <li>Digital forensic science and governance.</li> <li>A specialist subject of the student's choice in an area offered by the Programme at Level 6.</li> <li>How forensic and ethical hacking processes can be used to support information security</li> <li>The development of software or other IT solutions to security and digital forensic related problems.</li> <li>The professional, legal and ethical responsibilities of security personnel within the organisational, technical and global contexts in which information security is applied.</li> </ol>		<b>C – Subject-specific/Practical Skills</b> This programme provides opportunities for students to: <ol style="list-style-type: none"> <li>Retrieve, select and evaluate information from a variety of sources.</li> <li>Formulate a set of requirements for a security and/or digital forensics solution.</li> <li>Design a solution to a security and/or digital forensics related problem.</li> <li>Implement a solution to a security and/or digital forensics related problem.</li> <li>Evaluate a system or software with regards to security and/or digital forensics.</li> <li>Plan, monitor, and evaluate the progress of a security and/or digital forensics related project.</li> </ol>																					
<b>B – Intellectual Skills</b> This programme provides opportunities for students to: <ol style="list-style-type: none"> <li>Reason critically.</li> <li>Demonstrate independent thought.</li> <li>Analyse, interpret, synthesise and evaluate information.</li> <li>Identify and solve problems.</li> <li>Select and apply appropriate design methods to the solution of problems.</li> <li>Evaluate resource requirements of alternative solutions.</li> </ol>		<b>D – Transferable Skills</b> This programme provides opportunities for students to: <ol style="list-style-type: none"> <li>Structure and communicate ideas effectively, both orally and in writing.</li> <li>Learn independently in complicated contexts.</li> <li>Work professionally as an individual to develop creative solutions to problems.</li> <li>Work professionally in teams to develop creative solutions to problems.</li> </ol>																					