

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 with Digital Forensics – 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) G550 | HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load. 100376 (major), 100385 (minor) |
| External reference points <ul style="list-style-type: none"> • 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 Click here to enter text. | |
| Places of delivery Bournemouth University, Talbot Campus | |
| Mode(s) of delivery Full-time/Full-time sandwich | Language of delivery English |
| Typical duration UG September start (3 years full time with or 4 years full time with 30 weeks placement Sandwich placement) | |
| Date of first intake September 2023 | Expected start dates September |
| Maximum student numbers N/A | Placements 30 weeks, optional |
| Partner(s) N/A | Partnership model N/A |
| Date of this Programme Specification October 2023 | |
| Version number 1.0-0924 | |

Programme Specification – Section 1

| |
|---|
| Approval, review or modification reference numbers |
| E212216 |
| EC 2223 09 |
| EC 2223 32 |
| EC 2324 03 approved 09/10/2023 |
| Author |
| Dr Muntadher Sallal |

Programme Specification – Section 1

PROGRAMME STRUCTURE

| Programme Award and Title: BSc (Hons) Cyber security with Digital Forensics | | | | | | | | |
|--|-----------------|-------------------|-------------------------------|----------|----------|--|------------------------|--|
| Year 1/Level 4 | | | | | | | | |
| 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 | | | |
| Computer Fundamentals | Core | 20 | 50% | 50% | | 36 | 3.0 | 100734 100735 |
| Mathematics for Computing | Core | 20 | 50% | 50% | | 36 | 1.0 | 100400 |
| Programming | Core | 20 | 50% | 50% | | 36 | 1.0 | 100956 |
| Introduction to Cyber Security | Core | 20 | | 100% | | 36 | 1.0 | 100376 |
| Network Essentials | Core | 20 | | 100% | | 36 | 1.0 | 100365 |
| Computing and Society | Option | 20 | | 100% | | 36 | 1.0 | 100631 100367 |
| 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 | | | | | | | | |
|--|--------------------|-----------------------|--------------------------------------|--------------|--------------|--|-------------------------|---|
| 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 | | | |
| Ethical Hacking | Core | 20 | 50% | 50% | | 36 | 1.0 | 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 with Digital Forensics (requires 120 credits at Level 4 and 120 credits at Level 5) | | | | | | | | |
| Compulsory/Optional placement year in industry/business: Students who successfully complete the required compulsory 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. | | | | | | | | |

Programme Specification – Section 1

| Year 3/Level 6 | | | | | | | | |
|--|--------------------|-----------------------|--------------------------------------|--------------|--------------|--|-------------------------|---|
| 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 | | | |
| Digital Forensics | Core | 20 | | 100% | | 36 | 1.0 | 100385 |
| 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 |
| Software Quality Assurance | Option | 20 | | 100% | | 36 | 1.0 | 100374 |
| 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 with Digital Forensics | | | | | | | | |
| 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. | | | | | | | | |

Programme Specification - Section 2

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) Cyber Security and Digital Forensics is offered to provide for those particularly interested in a career involving cyber security and/or digital forensics. It is based on the premise that cyber security and digital forensics 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 with 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) Cyber Security & Digital Forensics 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. 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 to contribute 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).

Programme Specification - Section 2

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. This programme is a response to the great and immediate need for people with data science and advanced analytics expertise

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 Specification - Section 2

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/stage 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 Principles, techniques and concepts of cyber security and digital forensics</p> <p>A2 Enabling technologies for cyber security and digital forensics applications</p> <p>A3 A rigorous engineering approach to investigating and solving cyber security and digital forensics problems in business context</p> <p>A4 The management and development of IT solutions to address cyber security and digital forensics or other problems</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (A1 – A5); • seminars (A1 – A5); • directed reading (A1 – A5); • use of the VLE (A1 – A5); • independent research (for dissertation) (A1 –A5). |
| <p>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.</p> | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • open book examinations (A1-A5); • coursework essays (A1 – A5); • dissertation (A1-A5). |
| <p>B: Intellectual skills</p> <p>This programme/level/stage 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>B1 Critically thinking, problem-solving and decision-making to solve cyber security and digital forensics problems;</p> <p>B2 Analyse, interpret, synthesise and critically evaluate information from current research;</p> <p>B3 Critically evaluate and justify alternative approaches to solutions development;</p> <p>B4 Formulate, plan, execute, and report on a cyber security and digital forensics project involving original contributions;</p> <p>B5 Communicate findings to professional and academic standards.</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); • independent research (for dissertation) (B1 – B5). |

Programme Specification - Section 2

| | |
|---|--|
| | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (B1- B5); • coursework essays (B1 – B5); • dissertation (B1 – B5). |
| <p>C: Practical skills</p> <p>This programme/level/stage 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 Analyse, specify, design and implement cyber security and digital forensics applications to meet business goals;</p> <p>C3 Select appropriate methods and tools for solving cyber security and digital forensics problems;</p> <p>C4 Plan, monitor and evaluate the progress of a cyber security and digital forensics solution.</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (C1 – C4); • coursework essays (C1 – C4); • independent research for empirical dissertation (C1 – C4); • group exercises (C1 – C4). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (C1-C4); • coursework essays (C1-C4); • dissertation (C1- C4). |
| <p>D: Transferable skills</p> <p>This programme/level/stage 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>D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas.</p> <p>D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.</p> <p>D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (D1 – D4); • seminars (D1- D4); • use of the VLE (D1 – D4); • directed reading (D1- D4). |

Programme Specification - Section 2

| | |
|--|--|
| <p>D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.</p> <p>D5 Distill, synthesise and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere.</p> | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • coursework essays (D1 – D4); • open book examinations (D1 – D4); • dissertation (D1- D4). |
|--|--|

LEVEL 5/DipHE INTENDED LEVEL OUTCOMES

| | |
|--|--|
| <p>A: Knowledge and understanding</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>A1 Principles, techniques and concepts of cyber security and digital forensics</p> <p>A2 Enabling technologies for cyber security and digital forensics applications</p> <p>A4 The management and development of IT solutions to address cyber security and digital forensics or other problems</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (A1, A2, A4, A5); • seminars (A1, A2, A4, A5); • directed reading (A1, A2, A4, A5); • use of the VLE (A1, A2, A4, A5). |
| <p>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.</p> | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (A1, A2, A4, A5); • coursework essays/presentations (A1, A2, A4, A5); • coursework design and implementation (A1, A2, A4, A5). |
| <p>B: Intellectual skills</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>B1 Critically thinking, problem-solving and decision-making to solve cyber security and digital forensics problems;</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> |

Programme Specification - Section 2

| | |
|--|--|
| <p>B2 Analyse, interpret, synthesise and critically evaluate information from current research;</p> <p>B3 Critically evaluate and justify alternative approaches to solutions development;</p> <p>B5 Communicate findings to professional and academic standards.</p> | <ul style="list-style-type: none"> • lectures (B1 – B3, B5); • seminars (B1 – B3, B5); • directed reading (B1 – B3, B5) <p>use of the VLE (B1 – B3, B5).</p> |
| <p>C: Practical skills</p> <p>This programme/level/stage provides opportunities for students to:</p> | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (B1 – B3, B5); • coursework essays/presentations (B1 – B3, B5). • coursework design and implementation (B1 – B3, B5). <p>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level/stage learning outcomes:</p> |
| <p>C1 Retrieve, select and evaluate information from a variety of sources;</p> <p>C2 Analyse, specify, design and implement cyber security and digital forensics applications to meet business goals;</p> <p>C3 Select appropriate methods and tools for solving cyber security and digital forensics problems;</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (C1 – C3); • seminars (C1 – C3); • group exercises (C1 – C3). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (C1-C3); • coursework design and implementation (C1 – C3). |
| <p>D: Transferable skills</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>D1 Demonstrate problem solving skills and the application of knowledge across the discipline areas.</p> <p>D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.</p> <p>D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (D1 – D4); • seminars (D1 – D4); • use of the VLE (D1 – D4); • group exercises (D1 – D4). • directed reading (D1 – D4). |

Programme Specification - Section 2

| | |
|---|---|
| <p>D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.</p> | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (D1 – D4); • coursework essays/presentations (D1 – D4). • coursework design and implementation (D1 – D4). |
|---|---|

LEVEL 4/Cert HE INTENDED LEVEL OUTCOMES

| | |
|---|---|
| <p>A: Knowledge and understanding</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>A1 Principles, techniques and concepts of cyber security and digital forensics</p> <p>A4 The management and development of IT solutions to address cyber security and digital forensics or other problems</p> <p>A5 The professional, legal & ethical responsibilities of cyber security and digital forensics within the organisational, technical and global contexts in which cyber security and digital forensics are applied.</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (A1, A4, A5); • seminars (A1, A4, A5); • directed reading (A1, A4, A5). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (A1, A4, A5); • coursework essays/presentations (A1, A4, A5). • coursework design and implementation (A1, A4, A5). |
| <p>B: Intellectual skills</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>B1 Critically thinking, problem-solving and decision-making to solve cyber security and digital forensics problems;</p> <p>B2 Analyse, interpret, synthesise and critically evaluate</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (B1, B2, B5); • seminars (B1, B2, B5); |

Programme Specification - Section 2

| | |
|---|--|
| <p>B5 Communicate findings to professional and academic standards.</p> | <ul style="list-style-type: none"> • directed reading (B1, B2, B5). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (B1, B2, B5); • coursework essays/presentations (B1, B2, B5). • coursework design and implementation (B1, B2, B5). |
| <p>C: Practical skills</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>C1 Retrieve, select and evaluate information from a variety of sources;</p> <p>C3 Select appropriate methods and tools for solving cyber security and digital forensics problems;</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (C1, C3); • seminars (C1, C3); • group exercises (C1, C3). <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • examinations (C1, C3); • coursework essays/presentations (C1, C3). • coursework design and implementation (C1, C3). |
| <p>D: Transferable skills</p> <p>This programme/level/stage 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/stage learning outcomes:</p> |
| <p>D2 Gather, select, and analyse a range of experimental and fieldwork data and present professionally using appropriate media.</p> <p>D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.</p> | <p>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none"> • lectures (D2 – D4); • seminars (D2- D4); • use of the VLE (D2 – D4); • directed reading (D2- D4). |

Programme Specification - Section 2

| | |
|---|---|
| <p>D4 Demonstrate initiative, self direction and exercise personal responsibility for management of own learning.</p> | <p>Assessment strategies and methods (referring to numbered Intended Learning Outcomes):</p> <ul style="list-style-type: none">• coursework essays/presentations (D2 – D4).• coursework design and implementation (D2 – D4).• examinations (D2 – D4). |
|---|---|

Programme Specification - Section 2

Programme Skills Matrix

| Units | | Programme Intended Learning Outcomes | | | | | | | | | | | | | | | | | | |
|-------|---|--------------------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | | A 1 | A 2 | A 3 | A 4 | A 5 | B 1 | B 2 | B 3 | B 4 | B 5 | C 1 | C 2 | C 3 | C 4 | D 1 | D 2 | D 3 | D 4 | D 5 |
| L | Human Computer Interaction | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| | Digital Forensics | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| E | Systems Development | X | X | X | X | X | X | X | X | X | x | X | X | X | X | X | X | X | X | X |
| V | Software Quality Assurance | X | X | X | X | X | X | X | X | X | x | x | x | x | X | X | X | X | X | X |
| E | Digital Innovation and Transformation | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| | Data Visualisation and Storytelling | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| L | Individual Project | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| 6 | Digital Futures (Elective) | | X | | X | X | | X | X | | X | X | | | X | X | X | X | X | |
| L | Software Engineering | X | X | | X | X | X | X | X | | X | X | X | X | | X | X | X | X | |
| E | Ethical Hacking | X | X | | X | X | X | X | X | | X | X | X | X | | X | X | X | X | |
| | Security Operations (SecOps) | X | X | | X | X | X | X | X | | X | X | X | X | | X | X | X | X | |
| V | Technological Innovations in Cyber Security | X | X | | X | X | X | X | X | | X | X | X | X | | X | X | X | X | |
| E | Network and Cyber Management | X | X | | X | X | X | X | X | | X | X | X | X | | X | X | X | X | |
| L | Software Business (Elective) | | X | | X | X | X | X | | | X | X | X | X | | X | X | X | X | |
| 5 | | | | | | | | | | | | | | | | | | | | |

Programme Specification - Section 2

| | | | | | | | | | | | | | | | | | | | | |
|--|---|---|--|--|---|---|---|---|--|--|---|---|--|---|--|--|---|---|---|--|
| L E V E L 4 | Programming | X | | | X | X | X | X | | | X | X | | X | | | X | X | X | |
| | Computer 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 | |
| | Network Essentials | 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

| | |
|---|--|
| <p>A – Subject Knowledge and Understanding This programme provides opportunities for students to develop and demonstrate knowledge and understanding of:</p> <ol style="list-style-type: none"> 1. Principles, concepts and techniques of cyber security and digital forensics; 2. Enabling technologies for cyber security and digital forensics applications; 3. A rigorous engineering approach to investigating and solving cyber security and digital forensics problems in business context; 4. The management and development of IT solutions to address cyber security and digital forensics or other problems; 5. 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. | <p>C – Subject-specific/Practical Skills This programme provides opportunities for students to:</p> <ol style="list-style-type: none"> 1. Retrieve, select and evaluate information from a variety of sources; 2. Analyse, specify, design and implement cyber security and digital forensics applications to meet business goals; 3. Select appropriate methods and tools for solving cyber security and digital forensics problems; 4. Plan, monitor and evaluate the progress of a cyber security and digital forensics solution. |
| <p>B – Intellectual Skills This programme provides opportunities for students to:</p> <ol style="list-style-type: none"> 1. Critically thinking, problem-solving and decision-making to solve cyber security and digital forensics 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 and digital forensics project involving original contributions; 5. Communicate findings to professional and academic standards. | <p>D – Transferable Skills This programme provides opportunities for students to:</p> <ol style="list-style-type: none"> 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

The regulations for this programme are Bournemouth University's Standard Undergraduate Admission Regulations. [BSc \(Hons\) Cybersecurity with Digital Forensics | 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