**KEY PROGRAMME INFORMATION**

| | |
|---|---|
| **Originating institution(s)**<br>Bournemouth University | **Faculty responsible for the programme**<br>Faculty of Science and Technology |
| **Final award(s), title(s) and credit**<br>MSc Cyber Security – 180 credits (90 ECTS) | |
| **Intermediate award(s), title(s) and credits**<br>PGDip Cyber Security - 120 Credits (60 ECTS)<br>PGCert Cyber Security - 60 Credits (30 ECTS) | |
| **UCAS Programme Code(s) (where applicable and if known)**<br><br>N/A | **HECoS (Higher Education Classification of Subjects) Code and balanced or major/minor load.**<br>100376 Computer and Information Security (major)<br>100385 Computer Forensics (minor)<br><br>**CAH Code**: 11-01-04 Software Engineering<br>**Does this programme require ATAS:** NO |
| **External reference points**<br>The UK Quality Code for Higher Education (https://www.qaa.ac.uk/the-quality-code)<br>QAA Chapter A1: The national level (incorporating the Framework for Higher Education Qualifications (FHEQ) in England, Wales and Northern Ireland)<br>QAA Chapter A2: The Subject and Qualification Level (incorporating Masters Degree Characteristics)<br>CPHC Cybersecurity Principles and Learning Outcomes<br>CPHC/ISC Perspectives: Integrating Cybersecurity into Computer Science Curricula<br>CyBOK: The Cyber Security Body of Knowledge v1.1<br>United Nations Sustainable Development Goals (SDGs) | |
| **Professional, Statutory and Regulatory Body (PSRB) links**<br>N/A | |
| **Places of delivery**<br>Bournemouth University, Talbot Campus | |
| **Mode(s) of delivery**<br>Full-time (FT) | **Language of delivery**<br>English |
| **Typical duration**<br>12 months – September Intake<br>16 months – January intake | |
| **Date of first intake**<br>September 2025 | **Expected start dates**<br>September, January |
| **Maximum student numbers**<br>80 | **Placements**<br>None |
| **Partner(s)**<br>N/A | **Partnership model**<br>N/A |
| **Date of this Programme Specification**<br>April 2025 | |
| **Version number**<br>1.0-0925 | |
| **Approval, review or modification reference numbers**<br>E242510 | |

**Author**
Professor Nan Jiang, Dr Duncan Ki-Aries

## PROGRAMME STRUCTURE

**Programme Award and Title: MSc Cyber Security**

**Stage 1/Level 7**
Students are required to complete 7 core units

| **Unit Name** | **Core/ Option** | **No. of Credits** | **Assessment Element Weightings** | | | **Expected Contact hours per unit** | **Unit Version No.** | **HECoS Code** (plus balanced or major/ minor load) |
|---|---|---|---|---|---|---|---|---|
| | | | **Exam 1** | **Cwk 1** | **Cwk 2** | | | |
| Cyber Threat Intelligence | Core | 20 | | 100% | | 30 | 1.0 | 100376 (major), 100755 (minor) |
| Ethical Hacking | Core | 20 | | 100% | | 30 | 1.0 | 100376 |
| Infrastructure and System Security | Core | 20 | | 100% | | 30 | 1.0 | 100376 |
| Digital Forensics | Core | 20 | | 100% | | 30 | 1.0 | 100385 |
| Industrial Skills and Professional Issues (Cyber Security) | Core | 20 | | 100% | | 30 | 1.0 | 100962 (Major), 101090 (Minor) |
| IT Governance and Ethics | Core | 20 | | 100% | | 30 | 1.0 | 100374<br>100812 (Balanced) |
| Individual Masters Project | Core | 60 | | 100% | | 10 | 2.0 | 100367 (major), 100962 (minor) |

**Exit qualification:**
MSc Cyber Security requires 180 credits at Level 7

## AIMS OF THE DOCUMENT

The aims of this document are to:

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

## AIMS OF THE PROGRAMME

The MSc Cyber Security programme aims to equip graduates with the skills and knowledge needed to develop, manage, and operate secure and effective systems within complex modern organisations. The program explores the interplay between corporate strategy, business processes, cyber threats, and the broader societal impacts of cybersecurity.

Cybersecurity is a pressing global concern, with nations and organisations worldwide facing escalating threats. Initiatives such as the UK's Cyber Security and Resilience Bill, EU's Cybersecurity Act, the US Cybersecurity and Infrastructure Security Agency (CISA), and China's Cybersecurity Law demonstrate the international commitment to strengthening cybersecurity capabilities.

This programme cultivates a range of critical skills, including analytical thinking and problem-solving, essential for creating and maintaining secure systems. It covers both broad cybersecurity aspects, such as risk management, governance, ethics, and professional issues, and specialised skills like cyber threat intelligence, digital forensics investigation, and penetration testing.
By completing this programme, graduates will be well-equipped to pursue research and employment opportunities in cybersecurity-related fields, ultimately contributing to addressing the current cybersecurity skills gap and enhancing global cyber resilience.

The primary aim of this postgraduate programme is to develop Masters-level graduates who possess:

- A critical understanding of assurance methods, security, and risk management concepts necessary for supporting business processes and systems.
- A critical understanding of creating cutting-edge business risk analytics, interoperability of cross-domain solutions, and originality in applying knowledge and skills to manage security incidents and events.
- Technical skills and competencies to work with data (clear, encrypted, or transformed), secure information management, assured knowledge exchange, digital analytics, processes, technology, and architecture across various industries and segments, such as defence, critical national infrastructure, industry, and other related contexts.
- Research skills in areas including literature reviews, critical analysis of research findings, project proposals, planning, experiment design and analysis, and dissemination, with a focus on the application of these skills to cyber security topics.

## ALIGNMENT WITH THE UNIVERSITY'S STRATEGIC PLAN

The MSc Cyber Security programme aligns with Bournemouth University's 2025 strategic plan, which emphasizes the fusion of excellent teaching, world-class research, and professional practice. This alignment reflects the institution's core values of Excellence, Inclusivity, Creativity, and Responsibility.

Students in the programme benefit from the support of academics with extensive industry experience, many of whom are actively involved in various cybersecurity-related projects with external organisations. These academics are also engaged in cutting-edge research, and students are encouraged to participate in co-creation and co-publication projects.

The programme's pedagogical approach focuses on practical, industry-focused tasks, collaborative learning, and engagement with the industry through guest lectures, industrial events and projects. This approach aims to equip students with the full range of skills necessary to succeed in the contemporary cybersecurity environment. The academic team's own industrial experience, as well as their network of

industry contacts, informs the programme. These industry contacts may also contribute directly to the programme by delivering guest lectures.

## LEARNING HOURS AND ASSESSMENT

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

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

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. This programme adheres to best practice in both academia and industry. MSc dissertation projects can range from constructing an artefact to professional standards to conducting empirical research. Students will also produce concise reports similar to scientific papers, demonstrating rigorous research, analysis and presentation of results..

## 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 7 INTENDED PROGRAMME OUTCOMES

<table>
<tr><td>A: Subject knowledge and understanding<br><br>This programme/level provides opportunities for students to develop and demonstrate knowledge and understanding of:</td><td>The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes:</td></tr>
<tr><td rowspan="2">A1 Principles, concepts and techniques of cyber security and related research, at, or informed by the forefront of the area of study.<br><br>A2 Enabling technologies for cyber security-related applications within the discipline.<br><br>A3 A rigorous data-driven/engineering approach to investigating and solving current cyber security-related problems, within complex or unpredictable scenarios, such as those in defence, critical national infrastructure, industry, and other related contexts.<br><br>A4 The management and development of effective artefacts to address cyber security-related problems and management of risks.</td><td>Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):<br><br>• lectures (A1 – A5);<br>• seminars (A1 – A5);<br>• directed reading (A1 – A5);<br>• use of the VLE (A1 - A5);<br>• independent research (for project) (A1 - A5).</td></tr>
<tr><td>Assessment strategies and methods:<br>• coursework (A1 – A5);<br>• project (A1 - A5).</td></tr>
</table>

| | |
|---|---|
| A5 The professional, legal, and ethical responsibilities of security personnel – and of securing personnel, data, and systems within the organisational, technical, and global contexts in which cyber security and risk management approaches are applied. | |
| **B: Intellectual skills**<br><br>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: |
| B1 Critical thinking, problem-solving and decision-making to solve complex security-related problems with a high degree of autonomy.<br><br>B2 Analyse, interpret, synthesis, and critically evaluate concepts, principles and practices at the forefront of the area of study.<br><br>B3 Critically evaluate and justify alternative approaches to solutions development at the forefront of the area of study.<br><br>B4 Formulate, plan, execute, and report on a project demonstrating innovation and/or originality.<br><br>B5 Communicate findings to specialists and a diverse range of non-specialist audiences, adhering to professional and academic standards. | Learning and teaching strategies and methods (referring to numbered Intended Learning Outcomes):<br><br>• lectures (B1 – B3, B5);<br>• labs/seminars (B1 – B5);<br>• workshops (B1 – B5);<br>• use of the VLE (B1 – B3);<br>• independent research (for project) (B1 - B5).<br><br>Assessment strategies and methods:<br>• coursework (B1 - B5);<br>• project (B1 - B5). |
| **C: Practical skills**<br><br>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 Retrieve, select, and evaluate information from a variety of sources demonstrating originality in the application of knowledge.<br><br>C2 Analyse, specify, design, and implement effective and secure applications to meet business goals given complex or open constraints.<br><br>C3 Select appropriate methods and tools for solving cyber security-related problems and reducing risk within complex or unpredictable scenarios.<br><br>C4 Plan, monitor and evaluate the progress of a cyber security-related solution. | Learning and teaching strategies and methods:<br><br>• lectures (C1 – C3);<br>• labs/seminars (C1 – C4);<br>• workshops (C1 – C4);<br>• use of the VLE (C1 – C2);<br>• coursework (C1 – C4);<br>• independent research (for project) (C1 – C4);<br>• group exercises (C1 – C4).<br><br>Assessment strategies and methods:<br>• coursework (C1 – C4);<br>• project (C1 – C4). |
| **D: Transferable skills**<br><br>This programme/level/ provides opportunities for students to: | The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes: |
| D1 Demonstrate well-developed problem-solving skills and originality in the application of knowledge in the discipline. | Learning and teaching strategies and methods:<br>• lectures (D1 - D5); |

| | |
|---|---|
| D2 Gather, select, and analyse a range of experimental and fieldwork data, and present professionally using appropriate media.<br><br>D3 Structure and communicate ideas professionally and effectively, adhering to appropriate professional and academic standards.<br><br>D4 Demonstrate initiative, self-direction, and exercise personal responsibility for management of own learning in a proactive and effective manner.<br><br>D5 Distil, synthesise, and critically analyse alternative approaches and methodologies to problems and research results reported in literature and elsewhere. | • labs/seminars (D1- D5);<br>• workshops (D1 – D5);<br>• use of the VLE (D3 - D5);<br>• independent research (for project) (D1 – D5)<br>• directed reading (D1, D2, D4, - D5).<br><br>Assessment strategies and methods:<br>• coursework (D1 - D5);<br>• project (D1- D5). |

## PG Dip INTENDED LEVEL OUTCOMES

| | |
|---|---|
| **A: Knowledge and understanding**<br><br>This 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 Principles and techniques of cyber security and related research, at, or informed by the forefront of the area of study.<br><br>A2 Enabling technologies for cyber security-related applications within the discipline.<br><br>A4 The management and development of effective artefacts to address cyber security-related problems and management of risks.<br><br>A5 The professional, legal, and ethical responsibilities of security personnel – and of securing personnel, data, and systems within the organisational, technical, and global contexts in which cyber security and risk management approaches are applied. | Learning and teaching strategies and methods:<br>• lectures (A1, A2, A4, A5);<br>• seminars (A1, A2, A4, A5);<br>• directed reading (A1, A2, A4, A5).<br><br>Assessment strategies and methods:<br><br>• coursework (A1, A2, A4, A5). |
| **B: Intellectual skills**<br><br>This 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: |
| B1 Critical thinking, problem-solving and decision-making to solve complex security-related problems with a high degree of autonomy.<br><br>B2 Analyse, interpret, synthesis, and critically evaluate concepts, principles and practices at the forefront of the area of study.<br><br>B3 Critically evaluate and justify alternative approaches to solutions development at the forefront of the area of study. | Learning and teaching strategies and methods:<br>• lectures (B1 – B3, B5);<br>• labs/seminars (B1 – B3, B5);<br>• workshops (B1 – B3, B5);<br>• use of the VLE (B1 – B3).<br><br>Assessment strategies and methods:<br>• coursework (B1 – B3, B5) |

| | |
|---|---|
| B5 Communicate findings to specialists and a diverse range of non-specialist audiences, adhering to professional and academic standards. | |
| **C: Practical skills**<br><br>This 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 Retrieve, select, and evaluate information from a variety of sources demonstrating originality in the application of knowledge.<br><br>C3 Select appropriate methods and tools for solving cyber security-related problems and reducing risk within complex or unpredictable scenarios.<br><br>C4 Plan, monitor and evaluate the progress and operation of a cyber security project. | Learning and teaching strategies and methods:<br>• lectures (C1, C3);<br>• labs/seminars (C1, C3, C4);<br>• workshops (C1, C3, C4);<br>• use of VLE (C1);<br>• coursework (C1, C3, C4);<br>• group exercises (C1, C3, C4).<br><br>Assessment strategies and methods:<br>• coursework (C1, C3, C4); |
| **D: Transferable skills**<br><br>This level provides opportunities for students to: | The following learning and teaching and assessment strategies and methods enable students to achieve and to demonstrate the level learning outcomes: |
| D1 Demonstrate well-developed problem-solving skills and originality in the application of knowledge in the discipline.<br><br>D2 Gather, select, and analyse a range of experimental and fieldwork data, and present professionally using appropriate media.<br><br>D3 Structure and communicate ideas professionally and effectively to appropriate professional and academic standards.<br><br>D4 Demonstrate initiative, self-direction, and exercise personal responsibility for management of own learning. | Learning and teaching strategies and methods:<br>• lectures (D1 – D4);<br>• labs/seminars (D1- D4);<br>• workshops (D1 – D4);<br>• use of the VLE (D3 – D4);<br>• directed reading (D1, D2, –D4).<br><br>Assessment strategies and methods:<br>• coursework (D1 – D4). |

## PG Cert INTENDED LEVEL OUTCOMES

| | |
|---|---|
| **A: Knowledge and understanding**<br><br>This 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 Principles and techniques of cyber security and related research, at, or informed by, the forefront of the area of study. | Learning and teaching strategies and methods:<br>• lectures (A1, A4, A5);<br>• seminars (A1, A4, A5); |

| | |
|---|---|
| A4 The management and development of effective artefacts to address cyber security-related problems and management of risks.<br><br>A5 The professional, legal, and ethical responsibilities of security personnel – and of securing personnel, data, and systems within the organisational, technical, and global contexts in which cyber security and risk management approaches are applied. | • directed reading (A1, A4, A5);<br>• Independent research (for project) (A1, A4, A5).<br><br>Assessment strategies and methods :<br>• coursework (A1, A4, A5);<br>• project (A1, A4, A5). |
| **B: Intellectual skills**<br><br>This 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: |
| B1 Critical thinking, problem-solving and decision-making to solve complex security-related problems with a high degree of autonomy.<br><br>B2 Analyse, interpret, synthesis, and critically evaluate concepts, principles and practices at the forefront of the area of study.<br><br>B5 Communicate findings to specialists and a diverse range of non-specialist audiences, adhering to professional and academic standards. | Learning and teaching strategies and methods:<br>• lectures (B1, B2, B5);<br>• labs/seminars (B1, B2, B5);<br>• workshops (B1, B2, B5);<br>• use of the VLE (B1, B2).<br><br>Assessment strategies and methods:<br>• coursework (B1, B2, B5) |
| **C: Practical skills**<br><br>This 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 Retrieve, select, and evaluate information from a variety of sources demonstrating originality in the application of knowledge.<br><br>C4 Plan, monitor and evaluate the progress and operation of a cyber securityproject. | Learning and teaching strategies and methods:<br>• lectures (C1, C4);<br>• labs/seminars (C1, C4);<br>• workshops (C1, C4);<br>• use of VLE (C1);<br>• coursework (C1, C4);<br>• group exercises (C1, C4).<br><br>Assessment strategies and methods:<br>• coursework (C1, C4); |
| **D: Transferable skills**<br><br>This 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: |
| D2 Gather, select, and analyse a range of experimental and fieldwork data, and present professionally using appropriate media. | Learning and teaching strategies and methods:<br>• lectures (D2 – D4);<br>• labs/seminars (D2- D4); |

| | |
|---|---|
| D3 Structure and communicate ideas professionally and effectively, adhering to appropriate professional and academic standards.<br><br>D4 Demonstrate initiative, self-direction, and exercise personal responsibility for management of own learning in a proactive and effective manner. | • workshops (D2 – D4);<br>• use of the VLE (D3, D4);<br>• directed reading (D2 - D4).<br><br>Assessment strategies and methods:<br>• coursework (D2 – D4). |

## Programme Skills Matrix

| **Programme Intended Learning Outcomes**<br>**Units** | | **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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **L7** | Cyber Threat Intelligence | X | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| **L7** | Ethical Hacking | X | X | X | | X | X | X | X | X | X | X | X | X | | X | X | X | X | X |
| **L7** | Infrastructure and System Security | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| **L7** | Digital Forensics | X | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X | X |
| **L7** | Industrial Skills and Professional Issues (Cyber Security) | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| **L7** | IT Governance and Ethics | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| **L7** | Individual Masters Project | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |

## ADMISSION REGULATIONS

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

## 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 for a full list of approved Recognition arrangements and agreed entry criteria.

## ASSESSMENT REGULATIONS

6A – Standard Assessment Regulations: Postgraduate Taught Programmes.

## WORK BASED LEARNING (WBL) AND PLACEMENT ELEMENTS

N/A