Programme Specification for MSc Cyber Security

This document applies to Academic Year 2025/26 onwards

Table 1 Programme Specification for MSc Cyber Security

1.	**Awarding institution/body**	University of Worcester
2.	**Teaching institution**	University of Worcester
3.	**Programme accredited by**	N/A
4.	**Final award or awards**	PG Cert, PG Dip, MSc, MSc with Internship Pathway
5.	**Programme title**	MSc Cyber Security
6.	**Pathways available**	N/A
7.	**Mode and/or site of delivery**	Standard taught programme, delivered at the University of Worcester
8.	**Mode of attendance and duration**	Full time or Part time
9.	**UCAS Code**	N/A
10.	**Subject Benchmark statement and/or professional body statement**	This programme is informed by: QAA subject benchmark for Computing 2022 Cyber Security Body of Knowledge (CyBOK) CyBOK Mapping Framework for NCSC certified, BCS Academic Accreditation Guidelines, April 2022. It also meets the QAA Masters Degree Characteristics.
11.	**Date of Programme Specification preparation/ revision**	Approved March 2025

12. Educational aims of the programme

The MSc Cyber Security is designed for students who already hold a degree in a computing related discipline and are looking to specialise in cyber security. The course is tailored to meet the needs of both aspiring cyber security professionals, researchers and those looking to advance in this critical career.

The course equips students for professional mastery in cyber security and has the following features:

- Provide an intellectually challenging and vocationally relevant learning experience that incorporate the latest research and contemporary ideas in the Cyber Security profession.
- Progress students through structured learning that will give you an accessible introduction to computing practices and build on these to make you a confident Cyber Security professional, researcher and decision-maker.
- Provide a high-quality learning environment with teaching staff from a wealth of backgrounds including industrial and business applications, and advanced research establishments.
- Create practical experience in exploring contemporary Cyber Security issues and challenges in a real-world setting.
- Examine the ethical and societal impacts of Cyber Security applied to real-world problems.
- Provide highly relevant and employable skills in Cyber Security for the public and private sector.

13. Intended learning outcomes and learning, teaching and assessment methods

Table 2 knowledge and understanding outcomes and which module/code they relate to

Knowledge and Understanding

LO no.	On successful completion of the named award, students will be able to:	**Module Code/s**	**Award**
1	Apply relevant knowledge to critically evaluate applications of contemporary concepts, theories, and principles of cyber security.	COMP4009 COMP4010 COMP4006 COMP4012 COMP4030	*PG Cert, PG Dip MSc*
2	Identify and critically analyse contemporary problems and recent developments in cyber security threats, risks, and defences.	COMP4009 COMP4010 COMP4012 COMP4021 COMP4030	*PG Cert, PG Dip MSc*
3	Implement effective solutions to address complex real-world challenges through the creation systems that are secure by design.	COMP4009 COMP4010 COMP4012	*PG Cert, PG Dip MSc*

Table 3 cognitive and intellectual skills outcomes for module code/s

Cognitive and Intellectual skills

LO no.	On successful completion of the named award, students will be able to:	**Module Code/s**	**Award**
4	Analyse, apply and critically evaluate concepts, principles and practices at the forefront of the area of study, demonstrating insight and innovation, and application of these skills as appropriate	COMP4009C OMP4010CO MP4012CO MP4021CO MP4030	*PG Cert, PG Dip MSc*
5	Demonstrate innovation and/or originality, sophisticated judgement, critical thinking, research design and well-developed problem-solving skills with a high degree of autonomy, and to create comprehensive and highly effective approaches to identify, assess, and mitigate cyber security risks.	COMP4009C OMP4010CO MP4006CO MP4012CO MP4030	*PG Cert, PG Dip MSc*
6	Critically evaluate the legal, ethical, economic and social implications governing cyber security practices.	COMP4009C OMP4020CO MP4021	*PG Cert, PG Dip MSc*

Table 4 learning skills and capabilities related to employability outcomes for module code/s

Skills and capabilities related to employability			
LO no.	On successful completion of the named award, students will be able to:	**Module Code/s**	**Award**

Skills and capabilities related to employability			
7	Apply contemporary cyber security techniques within highly complex or unpredictable scenarios making insightful decisions given incomplete or missing data	COMP4010 COMP4012 COMP4021 COMP4030	*PG Cert,* *PG Dip* *MSc*
8	Evaluate secure systems and contemporary cyber security provision within highly complex or unpredictable scenarios, in a systematic and creative manner.	COMP4009 COMP4010 COMP4006 COMP4021 COMP4030	*PG Cert,* *PG Dip* *MSc*
9	Interpret the function and responsibilities of a variety of roles undertaken by cyber security practitioners.	COMP4009 COMP4012 COMP4020	*PG Cert,* *PG Dip* *MSc*

Table 5 transferable/key skills outcomes for module code/s

Transferable/key skills			
LO no.	On successful completion of the named award, students will be able to:	**Module Code/s**	**Award**
10	Demonstrate self-direction in tackling and solving complex problems, alongside approaching and implementing tasks and activities in a highly proactive and effective manner.	COMP4006 COMP4020	*PG Cert,* *PG Dip* *MSc*
11	Ability to communicate complex cyber security concepts and recommendations to specialist and non-specialist audiences in an accessible and impactful way.	COMP4006 COMP4021 COMP4030	*PG Cert,* *PG Dip* *MSc*
12	Reflect upon personal development to identify personal strengths and responsibility for sustained lifelong learning to stay abreast of emerging trends and best practices in cyber security.	COMP4020 COMP4021 COMP4030	*PG Dip* *MSc*

Learning, teaching and assessment

Teaching

Students are taught through a combination of interactive workshops, lectures, seminars and laboratory practical activities, fieldwork, etc. Interactive workshops take a variety of formats and are intended to enable the application of learning through discussion and small group activities. Seminars enable the discussion and development of understanding of topics covered in lectures, and laboratory practical activities are focused on developing subject specific skills and applied individual and group project work.

In addition, postgraduate students will be allocated a Personal Academic Tutor who is available who is available to offer academic support and guidance through the course.

The University places emphasis on enabling students to develop the independent learning capabilities that will equip them for lifelong learning and future employment, as well as academic achievement. A mixture of independent study, teaching and academic support from Student Services and Library Services, and also the Personal Academic Tutoring system enables students to reflect on progress and build up a profile of skills, achievements and experiences that will help them to flourish and be successful.

Contact time
In a typical week there will be at least 12 hours of timetabled teaching in lectures, seminars and small-group work. The precise contact hours will depend on the semester of study. For part time students, this will depend on the number of modules being taken. Typically, class contact time will be structured around:

- Delivery of theoretical content to address contemporary challenges in Artificial Intelligence.
- Practical in-class tasks relating theory to practice.
- Discussion and group activities.

Independent self-study
In addition to the contact time, full-time students are expected to undertake around 25 hours of personal self-study per week. Typically, this will involve completing online activities, reading journal articles and books, working on individual and group projects, undertaking research in the library and online, preparing coursework assignments and presentations, and preparing for examinations.

Independent learning is supported by a range of excellent learning facilities, including the Hive and library resources, the virtual learning environment, and extensive electronic learning resources.

Teaching staff
Students will be taught by a teaching team whose expertise and knowledge are closely matched to the content of the modules on the course. The team includes senior academics, professional practitioners with industry experience, demonstrators and technical officers.

Teaching is informed by research and consultancy, and many of our lecturers have a higher education teaching qualification or are Fellows of the Higher Education Academy.

Assessment
The course provides opportunities to test understanding and learning informally through the completion of practice or ‘formative’ assignments. Each module has one or more formal or ‘summative’ assessment which is graded and counts towards the overall module grade.

Assessment methods may include written examinations and a range of coursework assessments such as essays, reports, portfolios, performance, presentations and a final research project.

The precise assessment requirements for an individual student in an academic year will vary according to the modules taken, but a typical formal summative assessment pattern of the course is:

3 x written reports
1 x group project
2 x practical assessments
3 x presentations
2 x formal examinations of 2 hours duration
1 x research proposal
Major dissertation of approx. 15,000 words

Students will receive feedback on formative assessments and summative assessments. Feedback is intended to support learning, and students are encouraged to discuss this with personal academic tutors and module tutors as appropriate.

The course team will provide feedback on formal course work assessments within 20 working days of hand-in.

14. Assessment strategy

The assessment strategy for this course has been designed to provide students with challenges appropriate for Masters level modules. The programme is assessed through a range of summative practical coursework including presentations, software artifacts and reports. Formative feedback will be provided through a range of approaches including direct verbal and written feedback from tutors and interaction with peers. The overall purpose of the assessment strategy is to enable students to:

- Demonstrate that they have the intellectual rigour and subject knowledge commensurate with a course of this nature and have developed the analytical skills expected of Master Level study.
- Demonstrate the ability to synthesise appropriate theories, models and concepts from a range of modules studied on the course and apply them to critically evaluate real world scenarios.
- Gain experience in working individually and as part of a team.
- Produce concise documentation and effective presentation skills.
- Receive continuous, regular and appropriate feedback throughout the course

In designing the assessment strategy for the programme, the course team have been careful to align with the University's Assessment Policy, the University's Generic Grade Descriptors and the QAA Subject Benchmark Statement.

The course assessment methods are designed to effectively assess the achievement of learning outcomes which is why there is a range of assessment used throughout the modules. Each assessment is very well outlined in the module documentation, there is a standard approach for including a clear assessment brief outlining the task of the assignment as well as the grading criteria. Using assessment grids, with specific assessment criteria, is a standard practice across all assessment points on all modules. Assessment criteria/grade descriptors provided for each item are developed in line with University generic grade descriptors.

15. Programme structures and requirements

Table 6 award map for each level of the course

		Status Mandatory (M) or Optional (O)			
Module Code	**Module Title**	**Credits** (Number)	**PG Cert**	**PG Dip**	**MSc**
COMP4009	Cyber Threat Intelligence	15	O	M	M
COMP4010	Attack Detection and Forensic Analysis	15	O	M	M
COMP4006	Research Skills	30	O	M	M
COMP4012	Defensive Cyber Security	15	O	M	M
COMP4020	Digital Ethics, Security and Governance	15	O	M	M
COMP4021	Project Skills	30	O	M	M
COMP4030	Research Project	60	N/A	N/A	M
	Total Credits	180			

PG Certificate in Cyber Security To be awarded the PG Cert students must successfully complete 60 credits at Level 7.
PG Diploma in Cyber Security To be awarded the Masters, students must complete a total of 180 credits at Level 7 including 60 credits from the Research Project.
Masters (MSc) in Cyber Security To be awarded the Masters, students must complete a total of 180 credits at Level 7 including 60 credits from the dissertation.
Masters in Cyber Security with internship pathway Students must complete a total of 180 credits at Level 7 including 60 credits from the Research Project and undertake an internship of up to 12 months in duration on completion of the taught modules.

Full time students can finish the course in one year. Part time students would normally complete the course in no less than two years, but the maximum registration period is 6 years. Students have the option of selecting up to 90 credits of study per year, but the Research Project should be the final module taken.

16. QAA and professional academic standards and quality

This award is located at Level 7 of the OfS sector recognised standards and is design to meet the FHEQ Descriptor for a higher education qualification at level 7 (Master's degree). It is also aligned to the QAA Subject Benchmark statement for Computing (March 2022) and to take into account the QAA UK Quality Code for Higher Education.

17. Support for students

The Department of Computing, based within the Worcester Business School, offers students the best possible support to help them fully achieve their objectives. The following points exhibit the various dimensions of support provided for students:

- Course induction including a brief course overview, introduction to the delivery pattern and assessment for the programme and specific modules, introduction to the VLE and learning resources. The induction helps students to settle in and adjust to the new teaching and learning environment. It also helps them from the beginning to set the right expectations, so they are fully aware of the standards at Masters level.
- The virtual learning experience site, Blackboard, to provide learning resources and module information, exchange ideas and information between students and staff.
- Programme Leader as a point of contact for overarching programme questions and concerns.
- Course handbook (available via the VLE) incorporating module outlines, key contacts and guidance for assessments
- Allocated Personal Academic Support Tutor to help students' integration into the University, the requirements of the programme and make the best use of learning resources available and to provide a key contact for support
- Access to course information, module results via the student online learning environment (SOLE)
- Student Representation to ensure making students' voice heard and to provide feedback to the on-going process of course improvement
- Support for disabled students via Student Services and the Disability and Dyslexia Service

https://www2.worc.ac.uk/firstpoint/
https://www.worcester.ac.uk/life/help-and-support/services-for-students/home.aspx
https://www2.worc.ac.uk/disabilityanddyslexia/

18. Admissions

Admissions policy

The course seeks to recruit home and international individuals with existing computing experience who are looking to specialise in the field of cyber security.

The University of Worcester is an accessible place for higher education. It is committed to widening participation and encouraging diversity in the student population. Worcester Business School works closely with central student support services including the Admissions Office, the Disability and Dyslexia Service and the International Centre to support students from a variety of different backgrounds. We actively encourage and welcome people from the widest range of economic and cultural backgrounds and value the contribution of mature learners.

Entry requirements
The minimum standard entry requirement is an honours degree at 2:2 level in a computing or technology related subject, or for international students, computing or technology-related qualification recognised as an equivalent by the University of Worcester.

Computing or technology-related subjects might include:
- computing
- computer science
- computer engineering
- engineering
- information technology etc

Students who obtained their undergraduate degree outside of the UK are required to provide an IELTS certificate with an overall score of 6.5 or above and 5.5 in all subskills. https://www.worcester.ac.uk/study/International/international-applicants/english-language-requirements.aspx

See Admissions Policy for other acceptable qualifications.

Recognition of Prior Learning
Students with relevant previous study at postgraduate level or with extensive experience may be considered eligible for recognition of prior learning. Please contact the Registry Admissions Office for further information or guidance on 01905 855111.

Further information on Recognition of Prior Learning can be found at http://www.worcester.ac.uk/registryservices/941.htm

Admissions procedures
Entry to the course requires all applicants to complete an application form which gives a variety of information about the student's work experience, qualifications, and motivation. These will be checked by the Admissions Tutor. Where information on the form is insufficient for a decision to be made, the applicant will be requested to attend an interview with the Admissions Tutor.

19. Regulation of assessment
The course operates under the University's Taught Courses Regulatory Framework

Requirements to pass modules
- Modules are assessed using a variety of assessment activities which are detailed in the module specifications.
- The minimum pass mark is D- for each module.
- Students are required to submit all items of assessment in order to pass a module, and in some modules, a pass mark in each item of assessment may be required.

- Full details of the assessment requirements for a module, including the assessment criteria, are published in the module outline.

Submission of assessment items

- Students who submit course work late but within 7 days (one week) of the due date will have work marked, but the grade will be capped at D- unless an application for mitigating circumstances is accepted.
- Students who submit work later than 7 days (one week) will not have work marked unless they have submitted a valid claim of mitigating circumstances.
- For full details of submission regulations please see the Taught Courses Regulatory Framework.

Retrieval of failure

- A student is entitled to resit failed assessment items for any module that is awarded a fail grade.
- Reassessment items that are passed are capped at D-.
- If a student is unsuccessful in the reassessment, they have the right to retake the module (or, in some circumstances, take an alternative module); the module grade for a re-taken module is capped at D-.
- A student who fails 60 credits or more after exhausting all reassessment opportunities may be required to withdraw from the University.
- A student will be notified of the reassessment opportunities in the results notification issued via the secure student portal (SOLE). It is the student's responsibility to be aware of and comply with any reassessments.

Requirements for Awards

Table 7 requirements for awards

Award	Requirement
PG Cert in Cyber Security	Passed a minimum of 60 credits at level 7, as specified on the award map
PG Dip in Cyber Security	Passed a minimum of 120 credits at level 7, as specified on the award map
Masters (MSc) in Cyber Security	Passed a minimum of 180 credits at level 7, as specified on the award map
Masters (MSc) in Cyber Security with internship pathway	Students must complete a total of 180 credits at Level 7 including 60 credits from the Research Project, and undertake an internship of up to 12 months in duration on completion of the taught modules.

PG Cert and PG Dip awards are unclassified. The awards of Masters may be made with Pass, Merit or Distinction.

Classification of Masters

The classification will be determined by whichever of the following two methods results in the higher classification.

Method 1

a) Candidates will be awarded a Distinction where they have attained an average of A- (PD) or higher from the credit achieved with the University for the award.
b) Candidates will be awarded a Merit where they have attained an average of C+ (PM) or higher from the credit achieved with the University for the award.

Method 2

a) Candidates will be awarded a Distinction, irrespective of their other module results, where they have attained 90 credits at grade A- (PD) or higher
b) Candidates will be awarded a Merit, irrespective of their other module results, where they have attained 90 credits at grade C+ (PM) or higher

Candidates will be awarded a Pass where they have not fulfilled the rules for Method 1 or Method 2, but are eligible for the award of a Masters.

For further information on honours degree classification, see the Taught Courses Regulatory Framework.

20. Graduate destinations, employability and links with employers

Graduate destinations
The course will equip students with skills to pursue your career in Cyber Security and will also pave the way for studying this field at PhD level, should that be desired. Opportunities for Cyber Security professionals include:

- Cybersecurity Specialist
- Cyber Crime Analyst
- System Consultant
- Penetration and Vulnerability Tester
- Cyber Security Engineer
- Information Security Manager

Student employability
A range of opportunities are provided to enhance students' employability. Students will benefit from the close links that have been developed with local and national employers. This includes guest speakers, industry visit days and a project showcase event. Further careers guidance is available through the University of Worcester Career Advisory Service and periodic Career Fairs are organised by Student Services.

Strategies used to embed employability into the curriculum and enhance graduate employability within the Computing sector include:

- the integration of learning outcomes that meet key Graduate Attributes.
- access to a broad network of business managers and employers
- employment preparation includes mock interviews and meetings with employers
- projects defined in collaboration with industry partners
- a project showcase attended by industry partners
- opportunities to engage in real-world and practical activities throughout your course.

An optional internship (up to 12 months in duration) is available to all students, taking place on completion of the taught modules. This internship will not be credit-rated but will allow the student to gain first-hand experience within a real-world environment to enhance their future employability.

Links with employers
Worcester Business School aims to promote closer links with employers and has worked with a number of business clients in developing and delivering its programmes. This is supported by its Industry Advisory Group, which meets on a regular basis to inform the design and development of all of our Computing courses.

Industry partners also engage with our course at a more fine-grained level by providing guest speaker, industry visit days and contributions to final year projects.

These professional and business networks also involve external events, many of which are open to students, as well as employers. The school liaises with external agencies, such as the Institute of Directors, Federation of Small Businesses, Chamber of Commerce and Confederation of British Industry.

Please note: This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided. More detailed information on the learning outcomes, content and teaching, learning and assessment methods of each module can be found in associated course documentation e.g. course handbooks, module outlines and module specifications.