



Course information for applicants

This information applies to the course as it will be delivered to students starting the course in 2027/28.

Information provided here was confirmed on 24/08/2026

General information

Programme code

MCYBS

Target award

If you complete this course successfully you will be eligible for the award of:

MSc Cyber Security

Delivery mode

- ☒ On campus
☐ Distance learning

Where you will study

The majority of teaching will be at Headingley campus but on occasion may be at City campus.

Professional accreditation or recognition

Professional body

British Computer Society (BCS) - The Chartered Institute for IT

Provisional accreditation with the National Cyber Security Centre (NCSC) since 2021

Summary of the accreditation or recognition

A graduate meets some or all of the educational requirements for registration with BCS as a Chartered IT Professional (CITP). BCS will not accredit until graduates have exited the award.

The course has provisional accreditation with the National Cyber Security Centre (NCSC), this will be accredited when the graduate has exited the award.

Awarding body

Leeds Beckett University

Regulator

Office for Students

Level of qualification

Level 7 of the Framework for Higher Education Qualifications

Course duration

If you are made an offer of a place on the course, your offer letter will include the start date.

This course can be studied:

12 months, full-time (September start)

24 months, part-time (September start)

Part-time study

This course can be studied part-time.

If you study the course part-time, it will usually take twice as long to complete compared with the equivalent full-time course. The modules may be delivered in a different sequence than on the full-time course, but you will study the same modules as the full-time route.

Entry requirements

Admissions criteria are available on the online prospectus entry for this course.

If you have questions about entry requirements and admissions, contact AdmissionsEnquiries@leedsbeckett.ac.uk

Course fees

Course fees and a breakdown of any additional costs is included on the online prospectus entry for this course.

If you have questions about fees for this course, contact Fees@leedsbeckett.ac.uk

Timetable

You will receive your full timetable for the year during induction week.

What you will study

Course aims

This course aims to develop students to be able to implement Cyber Security mechanisms into any business they obtain employment with, including entering the Cyber Security profession. The course is intended for students who already have an IT background, from either a professional or academic route. It is not intended to be a course for experienced practitioners or students in Cyber Security.

Cyber security plays an important role in enabling the protection and trust required for business and society to effectively operate. Organisations and individuals increasingly depend on information and communications technology (ICT) infrastructure, which frequently processes and stores large amounts of sensitive data. Consequently, there is significant security risk involved, and ICT systems need to be defended against many types of malicious attack. Every new ICT solution or system has the potential to introduce vulnerabilities and be misused by

attackers. Therefore, organisations require security expertise to assess, design, deploy, and maintain security solutions.

The aims of the course are:

- To provide opportunities for graduates with an honours degrees in computing (or equivalent qualifications) to pursue advanced study in the field of Cyber Security and develop general skills appropriate to the holder of a Master's level award.
- To produce individuals who have a critical and balanced appreciation of the practical and theoretical issues associated with Cyber Security.
- To develop individuals who are equipped with the skills and knowledge to devise, develop, manage, and implement Cyber Security methodologies.
- To provide a forum for the exchange and critical analysis of information relating to the field of Cyber Security, thereby developing the experience and skills of the students themselves and contributing to the body of knowledge in relation to the cognate area of Cyber Security.

Teaching and learning activities

This is a very hands-on subject area where theory alone would be unlikely to allow a student to achieve successful employment in this field. Practical exercises allow for students to implement their theoretical learning and see how it relates to industry. Our in house built Hacktivity platform allows interaction with the practical side of the course for the onsite delivery.

Module material includes short, recorded lectures, lab and support documents which allow for clear guidance, screenshots and audio where appropriate to ensure students comprehension. In addition, online platforms are utilised through each module to encourage student to student, and student to staff, communication, fostering a community environment and enabling more inclusivity for students.

The VLE is the primary tool for delivering the study material with extensive links to other sites. The VLE is also the primary tool for submitting assessments – via TurnItIn. The VLE provides internal links to self-assessment activities, mainly quizzes, to enable students to check their own progress. The VLE will be used to post announcements and email students. All work will be placed here so that students will be able to access any resources made available. Students will be given the opportunity to demonstrate their learning through a variety of mechanisms including reports, presentations and practical undertakings.

The course utilises professional tools and guidelines from industry and professional bodies to inform the teaching methodologies and resources of the course. The course is structured to develop the students understanding of key concepts of theory and practical processes. The building of this knowledge and feedback for assessments undertaken by students allows a greater understanding of the subject area.

The course aims to foster the development of independent study skills and autonomy of learning and encourage a commitment to lifelong learning and continuous professional development. Teaching and learning methods increasingly promote the capacity for students to assume responsibility for their own learning and development. Progressive use of project based integrated assessment and product/problem-based learning allow students to take on greater self-direction of their learning.

Students must also develop subject specific skills that are marketable in the short to medium term as well as more general skills that will facilitate their future development and continuous learning. The course supports the latter through identification of appropriate skill sets and these are developed through the programme of study and assessment methods. In particular emphasis is placed on a student's ability to critically analyse the subject area and their ability to effectively communicate their understanding of the process.

The learning and teaching methods used are identified in the descriptor for each of the modules. These methods will promote the broad learning strategy of the University and the School, which are under constant review and refreshment. This is tested at least annually for fitness for purpose and integrity of the student learning experience for the award.

Course structure

This information is correct for students progressing through the course within standard timescales. If you have to repeat study or take time out during your course, you may be taught alternative modules which meet the overall course learning outcomes.

Level 7 (Full-time delivery)

Compulsory modules

Module title	Credits	Semester/teaching period
Cyber Security Landscapes	20	S1 / Year 1
Incident Response and Investigation	20	S1 / Year 1
Research Practice	20	S1 / Year 1
Ethical Hacking and Penetration Testing	20	S2 / Year 1
Web and Network Security	20	S2 / Year 1
Systems Security	20	S2 / Year 1
Dissertation	60	S3 / Year 1
Total number of credits of compulsory modules:	180	

Level 7 (Part-time delivery)

Compulsory modules

Module title	Credits	Semester/teaching period
Cyber Security Landscapes	20	S1 / Year 1
Ethical Hacking and Penetration Testing	20	S2 / Year 1
Web and Network Security	20	S2 / Year 1
Incident Response and Investigation	20	S1 / Year 2
Research Practice	20	S1 / Year 2
Systems Security	20	S2 / Year 2
Dissertation	20	S3 / Year 2
Total number of credits of compulsory modules:	180	

Assessment and feedback

Level 7

This course is assessed by a mix of coursework, exams / tests, presentations / demonstrations and practical assessments. There is a major independent study module which is assessed by a dissertation.

Workload

You can expect to spend a total of 100 hours learning per 10 credits.

Typically, a student on this course can expect to divide their time like this:

Overall workload	Level 7
Teaching, learning and assessment	234 hours
Independent study	1567 hours