LEEDS BECKETT UNIVERSITY

Course Specification

MSc Cyber Security

Course Code: MCYBS

2026/27

leedsbeckett.ac.uk

MSc Cyber Security (MCYBS)

Applicant Facing Course Specification for 2026/27 Postgraduate Entrants

Confirmed at

General Information

Award	Master of Science Cyber Security
Contained Awards	Postgraduate Diploma Cyber Security Postgraduate Certificate Cyber Security
Awarding Body	Leeds Beckett University
Level of Qualification and Credits	Level 7 of the Framework for Higher Education Qualifications, with 180 credit points at Level 7 of the Higher Education Credit Framework for England.
Course Lengths and Standard Timescales	Start dates will be notified to students via their offer letter. The length and mode of delivery of the course is confirmed below: • 12 months (full-time, campus based) • 24 months (part-time, campus based)
Part Time Study	PT delivery is usually at half the intensity of the FT equivalent course, although there may be flexibility to increase your pace of study to shorten the overall course duration. Some modules may be delivered in a different sequence to that defined within this information set but the modules offered within each level are consistent.
Location(s) of Delivery	The majority of teaching will be at Headingley campus but on occasion may be at City campus
Entry Requirements	Admissions criteria are confirmed in your offer letter. Details of how the University recognises prior learning and supports credit transfer are located here: https://www.leedsbeckett.ac.uk/student-information/course-information/recognition-of-prior-learning/ Admissions enquiries may be directed to: AdmissionsEnquiries@leedsbeckett.ac.uk.

Course Fees	Course fees are confirmed in your offer letter. A breakdown of any additional costs is included on the online prospectus entry for this course. Fees enquiries may be directed to Fees@leedsbeckett.ac.uk.

Policies, Standards and Regulations (https://www.leedsbeckett.ac.uk/our-university/public-information/academic-regulations/)

There are no additional or non-standard regulations which relate to your course.

Professional Accreditation or Recognition Associated with the Course

Professional Body

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

National Cyber Security Centre (NCSC) – provisional accreditation

Accreditation/ Recognition Summary

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.

Timetable Information

Timetables for Semester 1 will be made available to students during induction week via:

i) The Student Portal (MyBeckett)
ii) The Leeds Beckett app

Any difficulties relating to timetabled sessions may be discussed with your Course Administrator.

Key Contacts

Your Course Director	Dr Pip Trevorrow
Your Course Administrator	Jake Wrigglesworth - J.Wrigglesworth@leedsbeckett.ac.uk

Course Overview

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 course has obtained recognition through accreditation with both the National Cyber Security Centre (NCSC) (provisional) and the British Computer Society (BCS) – the Chartered Institute for IT.

The aims of the course are:

- To provide opportunities for graduates with an honours degree 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 Masters 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.

Course Learning Outcomes

At the end of the course, students will be able to:

1	Deal with complex problems and demonstrate critical evaluation of theoretical and practical issues associated with the implementation of Cyber Security methods and justify these based on ethical and legal requirements.
2	Demonstrate a critical analysis of current issues and new technologies within the field of Cyber Security.

3	Demonstrate originality in the application of knowledge and techniques to create and interpret knowledge in the area of Cyber Security.
4	Demonstrate originality and synthesis in the application of theory and techniques, drawn from earlier studies, through the production of the dissertation/project, a significant piece of high level independent work.

Teaching and Learning Activities

Summary

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.

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.

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 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.

Your Modules

This information is correct for students progressing through the programme within standard timescales. Option modules listed are indicative of a typical year. There may be some variance in the availability of option modules. Students who are required to undertake repeat study may be taught alternate modules which meet the overall course learning outcomes. Details of module delivery will be provided in your timetable.

Full Time Delivery

Level 7
Compulsory modules

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

Part Time Delivery

Level 7
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	60	S3 / Year 2
Number of credits of compulsory modules	180	

Assessment Balance and Scheduled Learning and Teaching Activities

The assessment balance and overall workload associated with this course are calculated from core modules and typical option module choices undertaken by students on the course. They have been reviewed and confirmed as representative by the Course Director but applicants should note that the specific option choices students make may influence both assessment and workload balance.

A standard module equates to 200 notional learning hours, which may be comprised of teaching, learning and assessment, any embedded placement activities and independent study. Modules may have more than one component of assessment.

Assessment

On this course students will be assessed primarily by coursework, with some elements of project work and a final dissertation and oral presentation.

Workload

Overall Workload	
Teaching, Learning and Assessment	241 hours
Independent Study	1559 hours