Cyber Security MSc Programme Specification

Academic Year:	2026/27
Degree Awarding Body:	The University of Bradford
Subject Benchmark:	Computing (Quality Assurance Agency 2019)
Qualifications Framework:	HE Qualifications of UK Degree Awarding Bodies (FHEQ: QAA 2014)
Target Degree Award:	Master of Science in Cyber Security [FHEQ Level 7]
Intermediate Awards:	Postgraduate Diploma or Postgraduate Certificate [FHEQ Level 7]
Programme Admissions:	September and January
Programme duration:	1 year full time; 2 years part time

This programme is accredited by the British Computing Society (BCS) - the Chartered Institute for IT, for the purposes of partially meeting the academic requirement for registration as a Chartered IT Professional (CITP). In association with the UK National Cyber Security Centre (NCSC/GCHQ), the award of MSc in Cyber Security is a provisionally certified postgraduate degree in cybersecurity.

Please note: The integrated ISO/IEC 27001 Lead Implementer and Lead Auditor Training is certified by the Professional Evaluation and Certification Board (PECB). PECB Certified ISO/IEC 27001 Lead Implementer/Lead Auditor are non-credit bearing professional certificates where the awards of Provisional Implementer/Auditor, Implementer/Auditor, Lead Implementer/Auditor or Senior Lead Implementer/Auditor are dependent on a student's professional experience. All students will take the required coursework that assesses these certificates. Students wishing to certify their learning for the optional award will need to pay an additional fee which is detailed on the course webpage.

Please note: The University has a set of terms and conditions for all students accepting an offer to study on a course here at Bradford. This is called the Student Contract. This document sets out the Terms and Conditions which apply when you accept an offer of a place on a programme of study at the University of Bradford. **View our Student Contract for further details.** Information about this programme and its modules has been published in advance of the academic year to which it applies. Every effort has been made to ensure that the information is accurate at the time of publication, but changes may occur given the interval between publishing and commencement of teaching. Any change which impacts the terms and conditions of an applicant's offer will be communicated to them.

Minor Modification Schedule

1. July 2025: Annual Changes for the 2025 academic year, including changes to academic regulation.
2. April 2026: Annual changes for the 2026 academic year, including inline links and reaccreditation by NCSC.
3. November 2026: Late publication

Introduction

Computers play such a fundamental part of our everyday life that is difficult to imagine what we would do without them. When computers and systems process private and personal information it is crucial that such information is protected. **Cyber Security** is necessary to prevent unauthorised access to the information that we store on our devices (computers, smartphones, tablets, etc.) and online, and defend ourselves against an ever-evolving host of cyber-attacks to, for example, online banking, social networks, businesses and critical infrastructure.

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.

This programme offers students the opportunity to develop a deeper understanding of cyber security as a discipline to gain an in-depth understanding of the issues faced by modern organisations. The **MSc Cyber Security** course covers developments in security with a firm base in academic research and offers the opportunity for students to study selected topics in advanced computer science, such as the additional qualification in Certified ISO/IEC 27001 Lead Implementer.

This programme meets a continued growing demand for cyber security specialists by offering individuals in current employment as well as recent graduates the best environment to enhance and develop their skills with advanced study of IT security, to equip them for senior technical and security management positions with organisations.

The focus within MSc Cyber Security on the principles, technologies and practices of cyber security helps students to gain the appropriate skills for future PhD studies and research careers as well as to become competent practitioners. The current programme curriculum ensures that all graduates have studied relevant security disciplines that reflect the aims of the United Kingdom Government Communications Headquarters (GCHQ) National Security Programme whilst adhering to the curriculum framework within the University of Bradford.

A professional and industry-informed programme

Students with relevant industry skills are encouraged to specialise in cyber security or refine and develop their existing expertise.

Our teaching is informed by industry in several ways. Staff undertaking KTP projects, national and EU funded research projects and consultancy work embed new knowledge and concepts into their teaching materials and curriculum planning, based on the research and development work they conduct.

Students get exposure to industry throughout their programme as this is embedded in a number of ways. Throughout the academic year industrial speakers deliver invited talks that inform and inspire our students about current and future developments within their disciplines. In addition, the industry qualification ISO27001 Lead Implementer is integral to the programme design.

Student societies with links to professional bodies afford further opportunities for our students to engage with industry, such as Pi Soc the first ever BCS Student Chapter, and our ACM student chapter. These societies are encouraged and supported by the School of Computing and Engineering to participate in industry led activities such as programming competitions, data dives and extra-curricular visits.

MSc Cyber Security at the University of Bradford

The University of Bradford has for many years successfully taught a range of information security programmes at undergraduate and postgraduate level. The MSc Cyber Security programme was originally introduced in 2004 and has run every year since then. This programme draws upon the successful research expertise of the School of Computing and Engineering from within the Faculty of Management, Sciences and Engineering in the University in addition to that within the Interdisciplinary Research Centre (IRC) in Cyber Security. This IRC has members from within Computer Science, Electronic Engineering, Civil Engineering, Peace Studies, Management, Law, Sociology and Psychology. This broad base of expertise and research is a fantastic resource for the continued development of the programme in cyber security.

The main goal of this MSc Cyber Security programme is to prepare professionally trained graduates for industry. In this respect, detailed discussions have taken place, initially with industry professionals, who along with all other stakeholders have had a major input into shaping the

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.

revised programme. Our Industry Advisory Board (IAB), with a membership comprised of industry representatives from both regional and national companies, meets twice a year to review our existing provision and to propose improvements to our courses.

Upon completing this programme, students will not only become experts on the Cyber Security issues faced by industry and the existing Cyber Security solutions, but they will also be able to develop new ones. This programme will give students the toolkit required to flexibly adjust as new cyber threats emerge.

Programme Aims

The MSc programme in Cyber Security is intended to respond to current academic challenges provided by increasing reliance on computers and networks for core business activity and to meet commercial needs for employees who are able to understand and think strategically about future developments in this area. The programme provides a high academic quality of service to students, covering both theoretical and practical aspects of computing, networking and cyber security. It enables students to equip themselves with knowledge, skills and understanding, at an advanced level within the chosen field of study.

On successful completion of the MSc Cyber Security students will have advanced knowledge of the principles and applications of network, computer and systems security through:

- **Systematic Understanding and a critical awareness at advanced level, of core computing, networking and security subjects including:**

A1 security technologies and a detailed understanding of the implications and issues relating to secure applications.

A2 recognition of the influence of the cyber world on secure system design and evaluation and application development for firewalls, authentication, encryption, certificates and security protocols.

- **Discipline Specific Skills, showing originality in the application of knowledge, together with a practical understanding of:**

A3 how established techniques of research and enquiry in security and cyber technologies are used to create and interpret knowledge in the discipline.

A4 the ability to design, implement, and evaluate secure systems.

A5 development of critical understanding of regulatory and practical issues relating to cyber security.

- **Personal and Transferable Skills necessary for employment requiring:**

A6 the exercise of initiative and personal responsibility.

A7 decision-making in complex and unpredictable situations.

A8 the independent learning ability required for continuing professional development.

Programme Learning Outcomes

To be eligible for the FHEQ Level 7 Certificate award, students will be able to:

1. Demonstrate an advanced understanding and application of some of the theories, principles and techniques applicable in the field of Cyber Security.

2. Demonstrate a systematic understanding and critical awareness of secure systems within an organisation and the technical, legal and business issues involved.

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.

3. Demonstrate a systematic understanding and critical awareness of the nature of a computer related crime and the people and organisations involved therein.

4. Demonstrate an advanced understanding of, and ability to apply concepts and principles underlying cryptographic primitives and protocols.

5. Demonstrate a comprehensive and critical understanding of techniques specific to the field of computer security.

Additionally, to be eligible for the FHEQ Level 7 Diploma award, students will be able to:

6. Critically analyse, model, construct and evaluate specific types of networks and be able to effectively implement a reliable and effective security protocol.

7. Select, adapt and apply the underlying technologies of secure systems.

8. Be proficient in the practical and theoretical concepts of computer science, current and emerging trends in technology.

Additionally, to be eligible for the FHEQ Level 7 Degree award, students will be able to:

9. Select, design, plan and manage a self-directed and managed research-informed project.

10. Demonstrate a critical awareness of current and possible future opportunities and problems in; Internet, Computer and System Security evaluating current developments and trends.

Learning and Teaching Strategy

Our Learning and Teaching Strategy is to provide a nurturing and supportive environment that enables students to become independent learners and problem solvers. For example, students receive formative feedback during lab sessions in order to identify areas for improvement. A personal academic tutor is assigned to each student to provide both academic and pastoral support. Team-based learning supports the student experience by utilising and enabling peer interaction and support.

The programme includes innovative and active learning methods. Throughout the programme, we make use of case studies so that students can apply their theoretical understanding to real-world issues. In this way, abstract concepts are brought to life through practical activities. We also use methods associated with the “flipped classroom” where content is outside the classroom leaving more time and space for activities and active learning within tutorial and lecture sessions.

We use Canvas to share course materials and reading lists, communicate with students, track student participation, facilitate discussions, support formative and summative assessments and provide feedback. Students can use Canvas independently to revise materials, ask questions and interact with lecturers and other students using discussions, practise and assess their understanding using quizzes, or for finding resources for further reading.

In addition to the standard technology enhanced learning approaches, we embed technologies to deliver key concepts in an interactive environment that strongly links theory with practical skills. For example, we link remotely with industry experts to deliver interactive sessions for developing student’s pen-testing skills.

Research active staff are involved in curriculum development based on their research activities, exposing students to the very latest and future developments within their field of expertise. We integrate knowledge and experience from Industrial partners through both our Industry Advisory

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.

Board and research projects through case studies, lab-based activities and invited talks, ensuring that research findings are at the heart of our curriculum.

The programme offers a curriculum with core elements in Cyber Security. Dissertation work further enriches the opportunities students have to take control of their own learning. A range of teaching and learning methods is employed including lectures, tutorials, laboratory work and directed private study. Each 20-credit module on the programme requires students to commit 200 hours of study. Some of these hours will be formally timetabled - lectures, laboratories, seminars, tutorials and workshops whilst others will involve students carrying out private study.

Four workshop sessions act as a springboard for consideration and integration of Legal Social Ethical and Professional (LSEPI) issues into the project work from its commencement. All students progressing onto the dissertation are required to attend these workshops. As part of the workshop series, seminar sessions will take place to introduce the concepts and wider context of LSEPI practices within the Computing discipline (e.g. analysis skills, the research process, dissertation outlines and managing projects, data protection, computer misuse, ethics etc.). The seminars define relevant terms and the implications for professional practice within Computing. These are followed by a tutorial session with a case study scenario for groups of students, and the members of staff supervising dissertations, to discuss and debate the various aspects of LSEPI practice that would impact upon the scenario and the possible decisions and hypothetical outcomes. The tutorial concludes with a plenary to discuss the wide variety of issues and viewpoints from the groups and the implications for their dissertation work.

To ensure these topics are developed within a students' dissertation period, these initial workshops will be strengthened through the requirement for students to discuss these issues with their supervisor on a one-to-one basis. In addition, students will be required to complete an Ethical Approval Form with the aim of highlighting any potential ethical and legal implications of the work proposed.

Equality, diversity, inclusion and ethics are embedded in our programme's learning and teaching activities. We celebrate differences and ensure that everyone has equal opportunities to achieve their desired outcomes. Students will be encouraged to explore a diverse range of digital technologies and theories, and engage constructively with businesses and communities to enrich their understanding of the impact of Cyber Security on everyone's everyday lives and embrace the values of equality, diversity and inclusion in their development of Cyber Security solutions. This approach will equip students with the wider perspective of the relevance of advance computing for Cyber Security for the betterment of businesses and society.

Assessment Strategy

Assessment for this programme is designed to develop skills in the area of cyber security in addition to more generic professional transferable skills such as team working, communication, leadership and decision making. The combination of group work, individual submissions, examinations, theoretical work and lab-based exercises helps develop skills that are essential in industry. Alongside gaining an MSc Cyber Security, students have the opportunity to gain the additional qualification in ISO/IEC 27001 Lead Implementer if they undergo additional assessment.

All our staff have achieved, or are working towards, Fellowship of the Higher Education Academy. As part of our commitment to Excellence in Learning and Teaching, we conduct research into innovative and effective teaching methods. For example, assessment for projects was enhanced by incorporating regular formative and summative feedback opportunities to enhance the final outcomes.

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.

Programme Structure and Curriculum

The MSc Cyber Security covers a range of specialist topics, leading to the qualification of a Master's degree with the option to study for additional industry qualifications.

Typically, a taught full-time Master's programme lasts for 12 months of full-time study (or 24 months part-time). Students admitted to the programme in September study in the semester pattern of 1,2,3. Students admitted in January study in the semester pattern of 2,3,1. Part time routes are available for both admission periods. Students on part-time routes can study the taught component in year 1 and complete the dissertation in year 2.

The relevance of the programme's content to the stated teaching aims and objectives is based on core computer science and informatics topics as well as modules on relevant cyber security in relationship to secure implementation of systems, and their application in practice. Students will have opportunity to enhance Personal Transferable Skills principally through participation in and taking responsibility for a major individual project.

The programme has two stages: the taught programmes stage which takes place during the first two semesters (or four semesters for the part-time route), and the project/dissertation stage. The taught programmes stage is organised on a modular basis. All modules are classed as Core modules and are assessed at FHEQ Level 7.

The programme has modules in the Autumn and Spring periods providing grounding and advanced study of the field. Students then have the opportunity to develop, through sustained major project work, advanced knowledge and understanding of cyber security.

Table 1: MSc Cyber Security Core Modules at FHEQ Level 7

Module Code	Module Title	Credit	Study Period
COS7052-B	Applied Cryptography	20	Autumn (Sem 1)
COS7030-B	ISO27000 Framework (ISMS)	20	Autumn (Sem 1)
COS7055-B	Network Security	20	Autumn (Sem 1)
COS7035-B	Business Systems Security	20	Spring (Sem 2)
COS7051-B	Cyber Physical Systems Security	20	Spring (Sem 2)
COS7029-B	Ethical Hacking	20	Spring (Sem 2)
COS7004-E	Dissertation	60	Full Year

Attainable Awards

Students will be eligible for the optional award of **ISO/IEC 27001 (Lead) Auditor** or **(Lead) Implementer** (Professional Evaluation and Certification Board) if they have successfully passed the coursework assessment of COS7030-B at 60% or higher and paid the additional course cost for certification detailed on the course webpage. All students doing so can receive the Provisional Implementer or Provisional Auditor certification, with advanced titles of Implementer/Auditor, Lead and Senior Lead dependent on their professional experience in information security.

Students will be eligible to exit with the award of **Postgraduate Certificate** if they have successfully completed 60 credits and achieved the award learning outcomes.

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.

Students will be eligible to exit with the award of **Postgraduate Diploma** if they have successfully completed 120 credits and achieved the award learning outcomes.

Students will be eligible for the **Degree** award of **Master of Science** if they have successfully completed 180 credits and achieved the award learning outcomes.

Assessment, Continuation and Award Regulations

This programme follows the Assessment, Continuation and Award regulations for postgraduate courses published on the University's website (**Regulation 9**).

Admission Requirements

We take into consideration a number of factors when assessing your application. It's not just about your grades; we take the time to understand your personal circumstances and make decisions based on your potential to thrive at university and beyond.

The standard entry requirements for the programme are typically an undergraduate degree classified at 2:2 or above in computer science, computer engineering, electrical engineering, informatics or other "computing-adjacent" subjects (including non-STEM disciplines such as finance, economics, etc. dependant on the modules taken) from an accredited degree awarding body. Candidates with non-STEM backgrounds have to demonstrate that they have studied at least two Mathematics or Computing related modules during their previous studies.

International students will need to meet the **University's standard entry requirement for English proficiency** as detailed on our website.

Applications are welcome from students with non-standard qualifications or mature students (those over 21 years of age on entry) with significant relevant experience. Candidates who do not fulfil the normal entry requirements but have extensive industrial experience in a related area are considered on an individual basis.

If applicants have prior certificated learning or professional experience which may be equivalent to parts of this programme, the University of Bradford has procedures to evaluate and recognise this learning to provide applicants with exemptions from specified modules or parts of the programme. Find more information about **recognition of prior learning decisions** on the University website.

If you are thinking of coming or have recently applied to the University of Bradford, don't wait until you have arrived to contact our Disability Service. We can arrange for you to talk to a member of our team about what support is on offer here at the University including an invitation to our Get Set Day. To contact the Disability Service please complete the **request support form**.

Information in this document is for the contemporary recruitment cycle and was accurate at time of publication. The current tariff and accepted qualifications for entry onto the programme is published at the online course page: **https://www.bradford.ac.uk/courses/pg/cyber-security/**

COPYRIGHT © 2026 THE UNIVERSITY OF BRADFORD.