University of Suffolk

DEFINITIVE COURSE RECORD

Course Title	**MSc Cyber Security**
Awarding Bodies	**University of Suffolk**
Level of Award[1]	**FHEQ Level 7**
Professional, Statutory and Regulatory Bodies Recognition	**None**
Credit Structure[2]	**180 credits at Level 7**
Mode of Attendance	**Full-time and Part-time**
Standard Length of Course[3]	**1 year full-time**
Intended Award	**MSc Cyber Security**
Named Exit Awards	**PgD Cyber Security** **PgC Cyber Security**
Entry Requirements[4]	**Standard Entry Requirements of undergraduate degree 2.2 Honours, any subject**
Delivering Institution(s)	**University of Suffolk**
UCAS Code	**TBC**

This definitive record sets out the essential features and characteristics of the MSc Cyber Security course. The information provided is accurate for students entering level 7 in the 2026-27 academic year[5].

Course Summary

The MSc Cyber Security is a postgraduate taught degree. It is a conversion course which is designed for students who do not have a computing undergraduate degree but who want to become experts in the field of cyber security. Graduates of this degree are likely to take up roles in industry and commerce as cyber security experts but could also progress to undertake PhD degrees perhaps using Cyber Security in combination with the domain of their original undergraduate subject.

Course Aims

The course aims are to:

1. Enable students, regardless of their first degree subject, to gain essential computing knowledge and skills, enabling them to advance deeper into the Cyber Security specialism.
2. Enable students to gain a deep comprehensive knowledge and systematic understanding of the advanced specialism of Cyber Security.

[1] For an explanation of the levels of higher education study, see the QAA Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies (2024)
[2] All academic credit awarded as a result of study at the University adheres to the Higher education credit framework for England.
[3] Where the course is delivered both full-time and part-time, the standard length of course is provided for the full-time mode of attendance only. The length of the part-time course is variable and dependent upon the intensity of study. Further information about mode of study and maximum registration periods can be found in the Framework and Regulations for Undergraduate Awards.
[4] Details of standard entry requirements can be found in the Admissions Policy and further details about Disclosure and Barring Checks (DBS) can be found on the University's DBS webpage.
[5] The University reserves the right to make changes to course content, structure, teaching and assessment as outlined in the Admissions Policy.

3. Enable students to apply the theory in practice, designing and developing robust quality architectures and computational solutions.
4. Enable students to derive meaningful insights from those solutions with a due appreciation for the uncertainties and unknowns associated with those insights.
5. Ensure that students are fully aware of the ethical and privacy dimensions of Cyber Security.

Course Learning Outcomes

The following statements define what students graduating from the MSc Cyber Security course will have been judged to have demonstrated to achieve the award. These statements, known as learning outcomes, have been formally approved as aligned with the generic qualification descriptor for level 7 awards as set out by the UK Quality Assurance Agency (QAA)[6].

Students who successfully complete this **level 7** course will have:

Knowledge and Understanding	Cognitive Skills	Subject Specific Skills	Key/transferable skills
A1. Expressed and employed comprehensive knowledge and systematic understanding of concepts, principles and theories, both established and emergent, relating to cyber security and computing	**B1**. Applied methods and techniques learned in cyber security to extend knowledge and understanding to realistic and real-world projects, developed critiques of them and, where appropriate, proposed new hypotheses.	**C1.** Deployed appropriate established and/or cutting-edge theory, practices and tools for the successful design, development, deployment and maintenance of computer-based security systems	**D1**. Developed a comprehensive ability to perform across several areas in cyber security, to a generalist level where they can critically evaluate and analyse possible solutions, design novel solutions and bring that solution to a successful conclusion in a defined time-frame, showing by doing so their capabilities and readiness for lifelong learning and professional training
A2. Expressed and employed comprehensive knowledge and systematic understanding of information security issues in relation to the design, development and the use of information systems	**B2.** Applied comprehensive knowledge, systematic understanding, and mastered techniques to initiate and execute their final-year project and multiple minor projects in different topic areas	**C2.** Recognised the legal, social, ethical and professional issues involved in the exploitation of cyber security technology and be guided by the adoption of appropriate professional, ethical and legal practices	**D2**. Evidenced the qualities and transferable skills necessary for postgraduate level employment requiring the exercising of initiative, personal responsibility, creativity and decision making, through working individually and in groups on mini-projects, extended case studies and scenarios, and their major project

[6] As set out in the QAA Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies (2024)

A3. Conceptual understanding of current research and advanced scholarship in cyber security, that enables a critical evaluation of the literature and that facilitates an appreciation of the associated uncertainties, ambiguities, and limits to knowledge at the forefront of the discipline.	**B3**. Critically evaluated arguments, concepts, requirements, constraints and data in order to make rational judgements on appropriate algorithms, designs, methods, and configurations leading to the necessary analysis, design, implementation, and/or testing of a solution or identification of a class of solutions to significant problems	**C3**. Researched, designed, implemented, tested, utilised and documented solutions to address specific problems, using their knowledge, understanding and technical skills in cyber security	
	B4. Presented ideas, information, analyses, designs, implementations, tests and results relating to cyber security, critically, comprehensibly and succinctly to both specialist and non-specialist audiences		
	B5. Demonstrated originality in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry are used to create and interpret knowledge in cyber security		

Course Design

The design of this course has been guided by the following QAA Benchmarks / Professional Standards:

1. The QAA Computing subject benchmark (2022) https://www.qaa.ac.uk/the-quality-code/subject-benchmark-statements/computing
2. QAA Masters Degree General Characteristics Statement 2020 https://www.qaa.ac.uk/docs/qaa/quality-code/master's-degree-characteristics-statement.pdf

University of Suffolk

DEFINITIVE COURSE RECORD

Course Structure

The MSc Cyber Security comprises modules at level 7.

Module Specifications for each of these modules is included within the course handbook, available to students on-line at the beginning of each academic year.

Module Title	Credits	Module Type[7]	Timing
Level 7 Modules			
Essential Topics in Computer Science	30	Requisite	Block 1
Information Systems Security	30	Requisite	Block 2
Penetration Testing and Hacking Humans	30	Requisite	Block 3
Forensics and Network Security	30	Requisite	Block 4
Masters Project (module code: IPLDSAM99)	60	Mandatory	Blocks 5 and 6

Awards

On successful completion of the course, students will be awarded a MSc Cyber Security. Students who leave the course early may be eligible for a Postgraduate Diploma in Cyber Security on successful completion of 120 credits, or a Postgraduate Certificate in Cyber Security on successful completion of 60 credits.

Course Delivery

The course is delivered at the DigiTech Centre at Adastral Park and on the Waterfront Campus. Students studying full-time on MSc Cyber Security are likely to have approximately 600 tutor structured learning hours. Tutor structured learning will be a mix of 240 class hours of lectures, seminars, tutorials and practical workshops and 360 hours of tutor-directed, asynchronous study such as research papers, videos and online material. Beyond this, students will normally be expected to undertake 100 hours of independent study for a single module, which would typically be around 17 hours in an average week but should be prepared for this to vary based on assignment deadlines and class exercises.

Course Assessment

A variety of assessments will be used on the course to enable students to experience and adapt to different assessment styles. With the exception of the Masters Project, each module will typically have a short summative assessment (which is graded and contributes to the overall degree classification) that will gradually build skills on a particular module, followed by a longer piece of summative assessment that will make use of the knowledge that has been built steadily. Each module also has several opportunities for formative feedback which will focus on both strengths and areas for improvement in each module (formative assessment does not count towards the degree classification). Group activities (non-assessed) will encourage peer learning and collaboration skills.

Course Team

The academic staff delivering this course are drawn from a team that includes teaching specialists and current practitioners. All staff are qualified in their subjects with their own specialist knowledge to contribute.

[7] Modules are designated as either mandatory (M), requisite (R) or optional (O). For definitions, see the Framework and Regulations for Postgraduate Awards

Course Costs

Students undertaking the MSc Cyber Security will be charged tuition fees as detailed below.

Student Group	Tuition Fees
Full-time UK	£10,400 per year
Part-time UK	£1,733 per 30 credits
Full-time EU/International	£16,550 per year
Part-time EU/International	£2,760 per 30 credits

Payment of tuition fees is due at the time of enrolment and is managed in accordance with the Tuition Fee Policy.

Academic Framework and Regulations

This course is delivered according to the Framework and Regulations for Undergraduate Awards and other academic policies and procedures of the University and published on the website.