University of Plymouth

Faculty of Science and Engineering

School of Engineering, Computing and Mathematics

Programme Specification

MSc Cyber Security

September Intake: 6566
January Intake: 7419

September 2025

1. MSc Cyber Security

The MSc Cyber Security (formerly MSc Computer and Information Security) is a one year programme consisting 120 credits of compulsory taught material and a 60 credit project.

Final award title:	**MSc Cyber Security** 180 Level 7 credits
Intermediate award titles:	**Postgraduate Diploma (PGDip)** 120 Level 7 credits
	Postgraduate Certificate (PGCert) 60 Level 7 credits
UCAS code	N/A
JACS code	**I100**

2. Awarding Institution: University of Plymouth

Teaching institution: University of Plymouth

3. Accrediting body

BCS – The Chartered Institute for IT

National Cyber Security Centre – Certified Degree

4. Distinctive Features of the Programme and the Student Experience

- The course gives students an appreciation of security in a broad context, emphasizing the need for a holistic approach to protection and information assurance.
- A dedicated security and forensics laboratory, purpose-built to represent a range of network topologies and monitoring conditions
- Opportunity to pursue industry-recognised certifications, such as EC-Council Certified Ethical Hacker (CEH), and AccessData Certified Examiner (ACE)

- It is underpinned by an active computer and information security research team within the Centre for Security, Communications and Network Research (CSCAN).

- It provides a basis from which candidates may progress to a research degree at MPhil or PhD level.
- This programme contains research-led project activities, leading to the production of research papers, which are combined into an annual published volume. Many project activities also go on to be published in peer-reviewed international conferences and journals.
- Linkage to professional and industry bodies, including Chartered Institute of Information Security and the BCS – The Chartered Institute for IT.

5. Relevant QAA Subject Benchmark Group(s)

Master's degrees in computing

6. Programme Structure

The programme is usually only offered as a full-time course. The course lasts for 12 months and leads at the end of this time to the award of Master of Science (MSc).

All modules are core, thus ensuring that all students are guaranteed a consistent experience in semesters of their coverage of the key discipline area. The programme consists of the following modules.

September intake

Semester 1 (60 credits)	Semester 2 (60 credits)	Summer
COMP5002 Security Operations & Incident Management	**COMP5003 (20 credits)** Ethical Hacking	**PROJ518 (60 credits)** MSc Dissertation and Research Skills
COMP5005 (20 credits) Security Architectures & Cryptography	**COMP5004** Digital Forensic & Malware Analysis	
COMP5006 (20 credits) Information Security Management & Governance	**COMP5011 (20 credits)** Cyber-Physical Systems Security	

January intake

Semester 1 (60 credits)	Summer	Semester 2 (60 credits)
COMP5003 (20 credits) Ethical Hacking		**COMP5002** Security Operations & Incident Management
COMP5004 Digital Forensic & Malware Analysis	**PROJ519 (60 credits)** MSc Dissertation and Research Skills	**COMP5005 (20 credits)** Security Architectures & Cryptography
COMP5011 (20 credits) Cyber-Physical Systems Security		**COMP5006 (20 credits)** Information Security Management & Governance

7. Programme Aims

The School of Engineering, Computing and Mathematics shares the values of the University of Plymouth and supports its mission through the provision of a range of courses relevant to the theory and practice of Information and Communication Technology.

1. To be informative and challenging, and to establish a knowledge base suitable for a career in Information and Communication Technology.
2. To give students with a variety of qualifications an opportunity to realise their potential.
3. To enrich curriculum content and teaching quality through the professional and/or research expertise of staff and through links with external organisations.
4. To encourage and support students whilst they develop and apply subject-specific and generic skills that will facilitate life long learning and continuing professional development.
5. To produce graduates and postgraduates who can make a significant contribution to their chosen profession.

In addition, the programme has the following specific aims:

1. To provide knowledge of the technologies for effective provision and management of computer and information security.
2. To produce a high level awareness of the issues arising from the need to protect computer and information systems and their associated assets.
3. To provide a broad grounding in security concepts and related standards, and a detailed understanding of the underlying technologies.
4. To provide an understanding of the computing and business issues related to computer and information security.
5. To provide an ability to follow a career in the computer and information technology and/or security industry, or in academic research.

8. Programme Intended Learning Outcomes

8.1. Knowledge and understanding

On completion graduates will have developed:

1. Personal, Professional and management techniques that are relevant to information technologists.
2. Detailed knowledge and understanding of the essential facts, concepts, principles and theories relevant to the design of secure systems and environments.
3. The professional and ethical responsibility of the information technologist in society.
4. The role of security within IT systems, and within the organisational settings they support.

8.2. Cognitive and intellectual skills

On completion graduates will have developed the ability to:

1. Plan, conduct and report a programme of original research.
2. Evaluate designs, processes and products and make improvements.
3. Integrate and evaluate data from a variety of sources.
4. Select and apply suitable computer based methods for modelling and analysing security problems.

8.3. Key and transferable skills

On completion graduates will have developed the ability to:

1. Communicate effectively in a variety of forms.
2. Manage resources and time.
3. Learn independently in familiar and unfamiliar situations

8.4. Employment related skills

On completion graduates will have developed the qualities and transferable skills necessary for employment as a computer and information security specialist requiring:

1. the exercise of initiative and personal responsibility;
2. a systems approach to decision-making in complex and unpredictable situations;
3. the independent learning ability required for continuing professional development.

8.5. Practical skills

On completion graduates will have developed the ability to:

1. Plan, execute a series of experiments and analyse experimental results to determine their strength and validity.
2. Prepare technical reports.

3. Research literature effectively.
4. Use computational tools and packages.

9. Admissions Criteria, including APCL, APEL and DAS arrangements

Entry requirements for the programmes are:

- An upper second class (2:1) honours degree or better in a computing or computing-related discipline;
- Applicants with a lower classification, or substantial industrial experience in lieu of formal qualifications may be considered subject to interview.
- A minimum IELTS English proficiency score of 6.5

No graduates of BSc (Hons) Cyber Security (formerly BSc (Hons) Computer and Information Security) from the University of Plymouth will be accepted.

The programmes adhere to the University regulations and guidelines for Accreditation of Prior Experiential Learning (APEL) and Accreditation of Prior Certificated Learning (APCL) for Masters programmes.

Students are required to produce evidence of English language ability. This will normally be the equivalent of GCSE Grade C or above in English language or IELTS average score of 6.5 or above with a score of at least 6.0 in the written component.

10. Progression criteria for Final and Intermediate Awards

- The MSc award requires 120 taught credits and 60 credit project, i.e., a minimum of 180 credits with a minimum mark of 50%.
- The PgCert award requires a minimum of 60 credits with a minimum mark of 50%.
- The PgDip award requires a minimum of 120 credits with a minimum mark of 50%.

The MSc award only, is categorised into three specific grades:

MSc with Distinction: This award is achieved by a student earning a mark of 70% and above, on both the overall programme, as well as the dissertation/major project.

MSc with Merit: This award is achieved by a student earning a mark of 60% and above, on both the overall programme, as well as the dissertation/major project.

MSc: This award is achieved by a student earning a mark of 50% and above, on both the overall programme, as well as the dissertation/major project

The programme adheres to the University's Postgraduate Taught Regulations: https://www.plymouth.ac.uk/student-life/your-studies/essential-information/regulations

11. Exceptions to Regulations

None

12. Transitional Arrangements

13. Mapping and Appendices:

13.1. ILO's against Modules Mapping

Intended Programme Learning Outcomes	Module
1. Knowledge and Understanding	
On completion, postgraduates will have developed:	
Personal, Professional and management techniques that are relevant to information technologists.	COMP5006
Detailed knowledge and understanding of the essential facts, concepts, principles and theories relevant to security design.	COMP5006, COMP5003, COMP5002, COMP5005, COMP5004 COMP5011
The professional and ethical responsibility of the engineer in society.	COMP5006, COMP5003 COMP5011

2. Cognitive and Intellectual Skills	
On completion, postgraduates will have developed the ability to:	
Plan, conduct and report a programme of original research.	PROJ518/519
Evaluate designs, processes and products and make improvements.	COMP5005, COMP5006, COMP5011
Integrate and evaluate data from a variety of sources.	COMP5003, COMP5005, COMP5004, COMP5011, PROJ518/9
Select and apply suitable computer based methods for modelling and analysing security problems.	COMP5003, COMP5002, COMP5004

3. Key and Transferable Skills	

On completion, postgraduates will have developed the ability to:	
Communicate effectively in a variety of forms.	COMP5006, PROJ518/9
Manage resources and time.	PROJ518/9
Learn independently in familiar and unfamiliar situations.	PROJ518 /9COMP5014

4. Employment related Skills	
On completion, postgraduates will have developed:	
The exercise of initiative and personal responsibility.	PROJ518/9
A systems approach to decision-making in complex and unpredictable situations.	PROJ518/9
The independent learning ability required for continuing professional development	COMP5005 COMP5006 COMP5002 COMP5003 COMP5004 COMP5011 PROJ518/9

5. Practical Skills	
On completion, postgraduates will have developed the ability to:	
Plan, execute a series of experiments and analyse experimental results to determine their strength and validity.	COMP5003, COMP5004, COMP5011, PROJ518/9
Prepare technical reports	COMP5004, PROJ518/9, COMP5011
Research literature effectively.	COMP5003, COMP5004,

	COMP5011, PROJ519
Use computational/simulation tools and packages.	COMP5003, COMP5002, COMP5005, COMP5004,
Give technical presentations	COMP5006

13.2. Assessment against Modules Mapping

Module Code	Module Title	Exam	Test	Coursework	Practice	Assessment
COMP5002	Security Operations and Incident Management			100%		
COMP5003	Ethical Hacking			100%		
COMP5004	Digital Forensics and Malware Analysis			100%		
COMP5005	Security Architectures and Cryptography			100%		
COMP5006	Information Security Management and Governance			80%	20%	
COMP5011	Cyber-Physical Systems Security			100%		
PROJ518	MSc Dissertation and Research Skills (September)			100%		
PROJ519	MSc Dissertation and Research Skills (January)			100%		

13.3. Skills against Modules Mapping

The figure below is a spreadsheet of skills mapped onto the BCS documentation.

Core Modules/ Accreditation Criteria (full wording for each criterion is available in Appendix IV of the Accreditation Guidelines)	COMP5006	COMP5003	COMP5002	COMP5005	COMP5004	COMP5007	PROJ518	COMP515	notes
Non-compensatable							✓	✓	
Core requirements for accreditation									
7.1.1 Critical review of literature	✓		✓	✓	✓	✓	✓	✓	
7.1.2 Development of the self-directed learner	✓	✓	✓	✓	✓	✓	✓	✓	
7.1.3 Respond to opportunities for innovation		✓	✓	✓	✓	✓	✓	✓	
7.1.4 Participate in the peer review process							✓	✓	
7.1.5 Undertake risk management	✓						✓	✓	
7.1.6 Use appropriate processes	✓	✓	✓	✓	✓	✓	✓	✓	
7.1.7 Investigate and define a problem	✓		✓	✓	✓	✓	✓	✓	
7.1.8 Apply principles of supporting disciplines	✓	✓	✓	✓	✓	✓	✓	✓	
7.1.9 An ability to work as a member of a development team						✓		✓	
Masters level requirements for CITP Further Learning									
8.1.1 Systematic understanding of knowledge of the domain with depth in particular areas	✓	✓	✓	✓	✓	✓	✓	✓	
8.1.2 Comprehensive understanding of essential principles and practices	✓	✓	✓	✓	✓	✓	✓	✓	
8.1.3 Understand and participate in the legal, social, ethical and professional framework	✓	✓	✓	✓	✓	✓	✓	✓	
8.2.1 Produce work informed by research at the forefront		✓	✓	✓	✓	✓	✓	✓	
8.2.2 Tackling a significant technical problem		✓	✓		✓	✓	✓	✓	
Additional requirements for CEng									
9.1.1 Systematic understanding of knowledge at the forefront in development and implementation of systems		✓	✓	✓	✓	✓	✓	✓	
9.1.2 Comprehensive understanding of the state of the art techniques		✓	✓	✓	✓	✓	✓	✓	
9.1.3 Understand and participate in the legal, social, ethical and professional framework in systems, software or information engineering	✓	✓	✓	✓	✓	✓		✓	
9.2.1 Develop and apply new technologies		✓		✓	✓	✓	✓	✓	
9.2.2 Show originality and innovation		✓		✓		✓	✓	✓	
9.2.3 Evaluation of commercial risk	✓	✓			✓		✓	✓	
Additional requirements for CSci									
10.1.1 Systematic understanding of knowledge at the forefront in computing science research			✓						
10.1.2 Comprehensive understanding of the scientific techniques									
10.1.3 Understand and participate in the professional, legal and ethical framework in computing science			✓						
10.2.1 Critical awareness of current research issues, problems and/or insights								✓	
10.2.2 Quantitative and qualitative research methods								✓	
10.2.3 Evaluation of scientific risk								✓	

13.4. Appendices

N/A