UNIVERSITY OF LONDON

Programme Specification 2024–2025

Cyber Security

MSc degree
PGDip
PGCert
Individual modules

Important document – please read

Contents

Important information regarding the Programme Specification

About this document

Last revised 27 March 2024

The Programme Specification gives a broad outline of the structure and content of the programme, the entry level qualifications, as well as the learning outcomes students will achieve as they progress. Some of the information referred to in this programme specification is included in more detail on the University of London website. Where this is the case, links to the relevant webpage are included.

Where links to external organisations are provided, the University of London is not responsible for their content and does not recommend nor necessarily agree with opinions expressed and services provided at those sites.

If you have a query about any of the programme information provided, whether here or on the website, registered students should use the '*ask a question'* button in the student portal. Otherwise, the *Contact Us* link at the bottom of every webpage should be used.

Terminology

The following language is specific to the Cyber Security programme:

Module: Individual units of the programme are called modules. Each module is a self-contained, formally structured learning experience with a coherent and explicit set of learning outcomes and assessment criteria.

Core module: A compulsory 15-credit module that must be taken.

Optional module: A 15-credit module that is chosen from a number of options. This applies solely to students registered on the PGCert or PGDip.

Study session: There are four study sessions in a year, each lasting 10 weeks. Sessions begin in October, January, April and July. Each session is following by an assessment submission point.

Resitting the assessment of a failed module: When you resit a failed module you will not be allocated a tutor group but you will have access to the learning materials on the VLE and you will be required to resubmit your summative assessment.

Repeating a failed module: When you repeat a failed module you will be allocated a tutor group, you will have access to the learning materials on the VLE and you will be required to resubmit your summative assessment.

Key revisions made

Programme specifications are revised annually. The quality committee of the member institution providing academic direction, as part of its annual review of standards, confirms the programme structure and the educational aims and learning outcomes, and advises on any development in student support. Where there are changes which may impact on continuing students, these are listed below. For all new students, the programme and general information provided in this document is correct and accurate and will be applicable for the current year.

Significant changes made to the Programme Specification 2024–2025

There are no significant changes to the Programme Specification 2024-25.

Programme title and awards

Postgraduate Degrees of the University of London may be classified. The award certificate will indicate the level of the academic performance achieved by classifying the award. The classification of the degree will be based on the ratified marks from the completed assessments.

The classification system for these awards is as follows:

Distinction; Merit; Pass.

Specific rules for the classification of awards are given in the Programme Regulations, under Scheme of Award

Programme title

Cyber Security

Qualifications

Master of Science in Cyber Security

Postgraduate Diploma in Cyber Security

Postgraduate Certificate in Cyber Security

Intermediate qualifications

Students may not normally request a lower intermediate qualification if studying on a higher qualification (except as an exit qualification) or accumulate these qualifications as they progress from lower to higher qualifications.

Exit qualifications

Postgraduate Diploma in Cyber Security

Postgraduate Certificate in Cyber Security

An exit qualification is an intermediate qualification, as noted above, for which the student may not have registered at the outset but which may be awarded on completion of specific modules (or credit accumulated) in a longer programme of study, if the student leaves the programme. Exit qualifications are awarded at the discretion of the Board of Examiners and once a student has accepted an exit qualification they will not normally be permitted to continue their study of the same award with the University of London.

Individual modules available for study on a stand-alone basis

There is also provision for select individual modules of the programme to be studied on a stand-alone basis without being registered for a related qualification, with the exception of the Project. Neither progression nor credit is automatic.

Award titles may be abbreviated as follows:

Master of Science – MSc

Postgraduate Diploma – PGDip

Postgraduate Certificate – PGCert

Level of the programmes

The Framework for Higher Education Qualifications of UK Degree-Awarding Bodies (FHEQ) forms part of the UK Quality Code for Higher Education of the Quality Assurance Agency for Higher Education (QAA).

The awards are placed at the following Levels of the Framework for Higher Education Qualifications (FHEQ):

MSc	Level 7
PGDip	Level 7
PGCert	Level 7

Relevant QAA subject benchmarks group

See the QAA website for information about quality assurance.

The QAA has not produced a benchmark statement for Cyber Security at postgraduate level.

Awarding body

University of London

Registering body

University of London

Academic direction

Royal Holloway, University of London

Accreditation by professional or statutory body

Not applicable

Language of study and assessment

English

Mode of study

Web supported learning with an online tutor.

Programme structures

The programme has two registration points in the year: October and April. There are four study sessions in a year, each lasting ten weeks. Sessions begin in October, January, April and July. Each session is following by an assessment submission point.

Students have an online induction session available through the virtual learning environment (VLE) prior to the start of their study session. This includes orientation of their learning environment and guidance on the structure and learning expectations for the module.

The MSc is a 180 UK credit degree programme. For the MSc, you must complete ten 15-credit core modules and one 30-credit Project module.

The PGDip is a 120 UK credit degree programme. For the PGDip, you must complete one 15-credit core module and seven 15-credit optional modules.

The PGCert is a 60 UK credit degree programme. For the PGDip, you must complete one 15-credit core module and three 15-credit optional modules.

Maximum and minimum periods of registration

The minimum periods of registration, from a student's effective date of registration, are:

	Minimum*
MSc	Two years
PGDip	One and a half years
PGCert	Six months

See the General Regulations for the maximum periods of registration for these qualifications.

*The minimum period of registration applies to students who enter the programme via Direct Entry, is subject to module availability and in some cases it may not be possible to complete within the minimum period of registration. Modules have been launched on a rolling basis since October 2022.

Students entering via the Performance-Based Admission entry route will progress at a slower rate to those who enter via Direct Entry. Full details can be found in Section 6 of the Programme Regulations.

In making a decision as to how many modules to register for in a given session, it is important to take account of on-going work and/or personal commitments

Credit value of modules

Further information about the credit systems used by universities in the UK and Europe is provided by the Quality Assurance Agency and the European Credit Transfer and Accumulation System.

Where credits are assigned to modules of a programme, credit indicates the amount of learning carried out in terms of the notional number of study hours needed, and the specified Framework for Higher Education Qualifications in England (FHEQ) credit level indicates the depth, complexity and intellectual demand of learning involved. The details below indicate the UK credits and the European Credit Transfer and Accumulation System (ECTS) values.

The MSc Cyber Security comprises a total of 180 UK credits (90 ECTS credits) at FHEQ level 7.

Recognition of prior learning

Recognition of prior learning is a generic term for the process by which we recognise and, where appropriate, award credit for learning that has taken place elsewhere, before entry onto this programme of study.

Where the prior learning covered a similar syllabus to a module/course studied elsewhere, credit will be awarded as if you took the Cyber Security module.

See the General Regulations (Section 3) for more rules relating to prior learning.

For this programme the University of London may recognise your prior learning and award you credit towards your qualification.

Entrance requirements

Applicants must submit an application in line with the procedures and deadlines set out on the website.

Entry route 1: Direct Entry

To qualify to register for the MSc, PGDip or PGCert you will need a bachelor's degree which is considered at least comparable to a UK second class honours degree from an institution acceptable to the University.

Entry route 2: Performance-Based Admissions

If applicants do not meet the requirements for Direct Entry they can apply for the MSc via the Performance-Based Admissions (PBA) route. To qualify for entrance via the PBA route you will need a third class bachelor's degree or Aegrotat.

Applicants with an appropriate professional experience qualification from a recognised professional body will be considered on an individual basis.

Students on the PBA route may transfer to the MSc on successful completion of two modules (30 credits).

Full details of the PBA route can be found in Section 6 of the Programme Regulations.

Entrance requirements for stand-alone individual modules

To qualify to register for a stand-alone individual module you will need a third class bachelor's degree or Aegrotat.

English language requirements

All applicants must satisfy the English language requirements for the programme. These are set out in detail on the programme page under the Requirements tab. All teaching is in English, therefore, students need to have the required level of written and spoken English to cope with their studies right from the start.

Additional information on English language proficiency tests is given on the website.

Where an applicant does not meet the prescribed English language proficiency requirements but believes that they can demonstrate the requisite proficiency for admission the University may, at its discretion, consider the application.

Further information on English language proficiency tests can be found on our website.

Computer specification and internet access

Students will require regular access to a portable computer with an internet connection to use the University of London's online resources and systems.

Students must be able to download and install software to their Windows or MacOS device to include secure examination browsers for online assessment purposes (if offered on their programme of study). Depending on the security settings for each assessment, students may be required to have full administrator rights on their computer to install and run the software needed to take part in the assessment. Full administration rights are likely to apply to a computer that they own but not to one provided by their employer, for example.

The portable computer must have at least the following minimum specification:

- Windows: 10 and 11 on 64-bit platforms
- MacOS Big Sur (version 11) and higher
- CPUs newer than 2011 (Intel Sandy Bridge (Core i3, i5 and i7 or newer))
- OpenGL 2.0 graphics driver
- Web camera & microphone (internal or external)
- A broadband internet connection capable of streaming video and a minimum of 0.15Mbps upload speed.

Minimum device requirements are subject to change and older operating systems may become obsolete over time.

It should also have the following applications installed:

- a word processor that accepts Microsoft Word formats (.doc and .docx)
- a PDF reader (e.g. Adobe)
- Microsoft Excel which can run macros
- a presentation program that supports Microsoft PowerPoint

Some modules/courses may have additional requirements such as video and audio recording options, Microsoft Excel, STATA, statistical or other specialist software. Where this is the case you will find information on the course webpages.

We are developing further security protocols and therefore students will require a mobile device (such as a mobile phone or tablet/iPad) to approve for our services. Full details, including specifications, will be provided ahead of the implementation.

Please note: full mobile access is not available for all programmes. Proctored assessments will not work on any smartphone, tablet, Chromebook, Linux Operating Systems or other mobile device of any kind.

Students with specific access requirements

The University of London welcomes applications from disabled students and/or those who have access requirements. The University will make every effort to provide reasonable adjustments to enable those with a disability, learning difficulty or access requirements to have the same opportunity as all other students to successfully complete their studies.

The University is committed to managing the application procedure and the programme itself to ensure that services are accessible for all students and that an inclusive environment is created. Students with a disability, or others who may need access arrangements to assist in taking examinations, should complete the relevant section of the application form, or contact the Inclusive Practice Manager. A separate room or other arrangements may be considered.

Requests are considered by a University panel, whose purpose is to ensure that students with disabilities and/or specific access requirements are neither advantaged nor disadvantaged by such arrangements when compared with other students. These considerations remain separate from the academic selection processes.

For further information, see Inclusive Practice Policy

Sources of funding and scholarships

Information about potential sources of funding and scholarships is updated annually and where available is included in the prospectus web pages.

For further information see the website.

Educational aims and learning outcomes of the programmes

Educational aims

The main educational aim of this programme is to offer a challenging, flexible scheme of study invigorated by research and industry insights, which advances students' ability to develop academic and practical insights into the subject of cyber security. It is intended that students will be encouraged to develop a broad range of transferable and technical expertise using their initiative and by thinking out problems themselves.

A student who passes the modules will have the essential introduction to a variety of methods, approaches and concepts in cyber security. Students will know how various organisations solve problems of security management, the major cryptographic mechanisms and how they can be applied and how computer systems and networks are made secure. Students will be introduced to a wide range of security techniques and they will be able to analyse the suitability of these techniques for a particular context.

MSc students will be able to apply the skills and knowledge they have learnt to a particular problem and produce a persuasive project report.

The programmes aim to:

- encourage independent critical and evaluative skills, and intellectual curiosity for life-long learning;
- cultivate a capacity to think critically about how organisations manage security;
- expand knowledge and understanding of the main security issues, for example, in the development of the Internet, web based services, the enterprise and consider a range of activities including protection of critical infrastructure;
- promote analytical engagement with the technical, legal and commercial issues in cyber security;
- encourage students to relate the academic study of security to practical issues of public, business/commercial and national concern;
- facilitate self-development of students into professionally organised and interactive individuals by practising skills of selection, assimilation and communication;
- enable students to understand and apply the concepts, approaches and methods in Cyber Security to a particular problem and produce a well-structured, informative and insightful report (MSc students only).

Learning outcomes: MSc Cyber Security

These learning outcomes indicate what a typical student might reasonably be expected to achieve and demonstrate if they take full advantage of the learning opportunities provided. More detailed information on the specific learning outcomes, content and the learning and teaching and assessment methods of each module can be found on the course web pages.

A student will be able to demonstrate:

- A systematic understanding and a critical awareness, much of it at the forefront of the discipline;
- A comprehensive and practical understanding of many key areas in cyber security;
- The ability to evaluate current research, industry trends and methodologies;
- Originality in the application of knowledge;
- The independent learning required for lifelong and continuing professional development.

A Knowledge and understanding

A student is expected to:

- Demonstrate a breadth of knowledge and understanding in the discipline of cyber security and work with key cyber security concepts and definitions;
- Understand the role and importance of cyber security in society;
- Consider the legal, ethical, and social implications of cyber security and the design and technology decisions that are made;
- Develop an understanding of risk management, its fundamental place in cyber security and how it influences decision making;
- Understand the principles of cryptography and how it is used to create and deploy security services and meet the challenges arising from societal use of cryptography;
- Appreciate the key security threats and risks faced in computer systems, networks and infrastructure and consider the techniques that can be used to provide security services and countermeasures;
- Recognise the role of standards, regulations, law and policy in cyber security; from computer systems, networks and infrastructure, in the context of organisation and government, including regulations and policies for data protection and privacy;
- Explain the importance of security in the development of applications, the importance of the secure software development lifecycle, identify issues relating to software security, their effect on the security of computer systems, and understand the threat posed by malicious software;
- Show a systematic understanding of digital networks and their operation, the security problems in networked, cyber-physical systems and critical infrastructure;
- Demonstrate a comprehensive understanding of the role of security mechanisms for modern computer systems, including hardware and software, and the operation of a range of access control, authentication mechanisms, and virtualisation;

- Understand aspects of civil and criminal law in cybercrime and recommended in the international cybercrime convention, and the mechanisms used to prevent, investigate or mitigate cybercrime;
- Appreciate the role of individuals to the fulfilment of information security goals, appreciate societal dynamics relating to security perceptions and practices and the limitations and considerations of policy implementation, training and behavioural interventions;
- Consider the cyber security career pathways and show **a** knowledge of major professional bodies in cyber security.

B Cognitive skills

- Identify the social, legal, ethical, and organisational implications of cyber security;
- Apply reasoning through abstract concepts and skills to solve security problems;
- Apply critical thinking to solve a specific security task;
- Conduct a critical analysis of professional articles, and research papers;
- Act autonomously in planning, solving, and implementing tasks at a professional level;
- Plan, execute, and complete a substantial project involving independent study over several months;
- Contribute to the development of an Information Security Management System (ISMS), by considering security policies, risk assessments, the selection, implementation and management of security controls, though to developing and documenting processes and procedures and the development of staff cyber security training and awareness programmes and materials;
- Identify how to support cryptography within a wider cyber security architecture and conduct a high-level analysis of cryptographic based services and justify design decisions;
- Consider attack models and approaches, methodologies and management of security/ penetration testing, demonstrating how a set of vulnerabilities may be exploited;
- Demonstrate knowledge of computer systems security including access control, authentication, and virtualisation;
- Demonstrate a critical appreciation of the trends that are likely to influence cyber security;
- Examine the motivation and methodologies of attackers and identify and evaluate trends in cybercrime, the techniques used and hacking methodologies;
- Identify key standards to support the implementation of data privacy; use privacy case studies to understand how privacy should be implemented;
- Examine the methodologies by which security behaviour can change and understand the underlying theories behind these methodologies.

C Practical and professional skills

- Manage learning and development, including time management and organisational skills;
- Apply knowledge and skills about cyber/information security to a particular problem, which may be of a professional, engineering, or academic nature;
- Compare different approaches, technologies and techniques to make informed decisions to solve cyber security problems;
- Plan a project, identifying tasks or work packages, deliverables, risks and dependencies;
- Undertake a literature review and apply referencing and citing in reports;
- Discuss and select research methods that can be applied to research or professional projects;
- Consider ethics in cyber security and research;
- Apply a number of statistical and qualitative analysis techniques to data and consider appropriate representation of data and results;
- Demonstrate independent work on a security-related project, for which the student has defined the objectives and rationale and present their work using reports;
- Demonstrate a critical understanding of security; its services, architecture and design across a range of scenarios; including experience of cryptographic algorithms, networks and protocols, computer systems and technologies in the context of cyber security;
- Design security-related systems, processes and procedures; including consideration of usable security and mitigating biases that affect individuals when taking security decisions;
- Consider standards, regulations, legal, ethical and societal concerns, in the context of cyber security;
- Develop, implement and evaluate security awareness programs and security behaviour change approaches.

Learning outcomes: PGDip Cyber Security

Students who are granted the PGDip will be expected to have passed one core 15-credit module and seven 15-credit modules from a choice of nine (120 credits total). As such, students obtaining this qualification should have gained sound understanding of the learning outcomes listed above for the MSc as relevant for the modules chosen.

Learning outcomes: PGCert Cyber Security

Students who are granted the PGCert will be expected to have passed one core 15-credit module and three 15-credit modules from from a choice of nine (60 credits total). As such, students obtaining this qualification should have gained sound understanding of the learning outcomes listed above for the MSc as relevant for the modules chosen.

This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if they take full advantage of the learning opportunities provided. More detailed

information on the specific learning outcomes, content and the learning, teaching and assessment methods of each module can be found in the module syllabuses.

Learning, teaching and assessment strategies

The core principles of the learning, teaching and assessment strategy for this programme are outlined below.

Principle 1: Ensuring students are prepared for study

An online induction will ensure that they are prepared for study and are familiar with the learning environment and sources of support during their student journey.

Principle 2: An engaging and vibrant learning environment

All students will have access to an online virtual learning environment (VLE) with learning support and tools enabling them to monitor their progress, assessing fulfilment of learning outcomes and development of skills-based outcomes throughout the curriculum. The VLE will provide a framework for the level of support selected by students.

Principle 3: Learning content

The learning content will be designed to provide students with opportunities to engage, and encourage reflective and deep learning, with accessibility a key feature to enable students to study across a range of mobile and media channels.

Principle 4: Student support

All students will have access to the Virtual Learning Environment, learning content, UoL Online library, tools and activities related to their chosen programme of study. Students will be supported by online tutors.

Principle 5: Flexibility

To facilitate the requirements of a diverse global community of learners, a core feature of this programme is flexibility in the design of the curriculum, providing for modules to be studied as on a modular basis facilitating student progress at a pace suitable to their circumstance.

Principle 6: Assessment

A core feature of this programme will be a varied range of learning activities embedded within the learning content for each module, designed to provide feedback to students on their progress towards learning outcomes. Summative assessment methods will be designed to promote retention of knowledge, providing encouragement through tutor feedback, with as wide a range of methods as possible to most effectively assess learning outcomes, within the context of the need for secure and reliable techniques appropriate to flexible learning.

Principle 7: Staff Development

The design, development and delivery of this programme will be supported with training for:

- Academic teams involved in the development of the materials and assessment;
- Module Leaders;
- Online tutors

Assessment methods

All assessments are submitted online via a University of London platform. Students must ensure that their device is kept up to date and complies with University Computer Requirements. Online examinations are proctored remotely except for students who study at a Recognised Teaching Centres for which examinations are normally held at established examination centres worldwide.

Each module is run over a 10 week block, with the exception of the Project which is run over two 10-week blocks.

All 15-credit modules are assessed by one element of assessment (100%), either coursework or an online examination.

The Project module (30 credits) is assessed by one element of assessment, a project report (100%).

Resits may be taken once the module results have been confirmed by the Board of Examiners.

Coursework is submitted in the VLE by prescribed deadlines.

An examination is defined as an element of assessment that takes place in a controlled environment. Students will be given details of how the modules on their programme are assessed, the specific environment or location that is permitted and the time allowed for the assessment.

Student support and guidance

Key features of the support for students include:

- Student Portal: for accessing student induction, study skills support, careers and employability resources, student wellbeing advice.
- University of London Careers Service – offers tailored careers and employability support to students whatever their course, wherever they are studying, and whether they are starting, developing, or changing their career. Support includes webinars led by careers consultants, employer and alumni panel events and a range of online careers resources.
- Student induction resources.
- Student Guide: This provides information which is common to all students and gives guidance on a range of issues from the start of a student's relationship with the University of London through to their graduation.
- VLE containing: self-assessment and student planner tools; comprehensive learning materials; e-resources/e-library; student forums and progress monitoring tools
- Online student advisor and online tutor
- Programme Regulations.
- The Online Library: This provides a range of full-text, multidisciplinary databases where journal articles, book reviews and reports can be found.

- A University of London email account and web area for personal information management.

Quality evaluation and enhancement

The University of London delivers the majority of its online and distance learning programmes through a collaboration between the University of London Worldwide and University of London federation members. However, some of the online and distance learning programmes draw solely on academic input from the University of London and are delivered without academic lead by a federation member. The policies, partnerships (where applicable) and quality assurance mechanisms applicable for the programmes are defined in the following key documents: The Quality Assurance Schedules, Guidelines for Examinations, General Regulations and, for each programme, programme specific regulations.

Awards standards

All University of London qualifications must comply with the Office for Students' (OfS) Conditions of Registration relating to quality and standards, which includes condition B5 (sector-recognised standards). This is to ensure appropriate standards for each qualification. In addition, every online and distance learning programme that is developed by a federation member of the University of London (or a consortium with representation by more than one federation member) will be developed to the same standard as would be applied within the institution concerned. Proportionate and robust approval procedures, including external scrutiny and student engagement, are in place for all programmes. Learning materials are written and all assessments are set and marked by academic staff who are required to apply the University's academic standards.

Review and evaluation mechanisms

Some of the key mechanisms in place to assure the standards of all University of London qualifications and the quality of the student experience, include:

- Annual programme reports: produced for all programmes in order to review and enhance the provision and to plan ahead;
- Independent external examiners: submit reports every year to confirm that a programme has been assessed properly and meets the appropriate academic standards;
- Annual student performance, progression and completion statistics
- Periodic programme reviews: carried out every 4-6 years to review how a programme has developed over time and to make sure that it remains current and continues to provide a good student experience.

Enhancements are made as necessary to ensure that systems remain effective and rigorous.

Student feedback and engagement

The principal channel for collecting feedback from students is the Student Experience Survey. Carried out every year, this collects feedback from the student body on a range of topics relating to the student lifecycle. The results are analysed externally and then considered in a number of different ways, including by the programme team, principal

committees and the senior leadership team. Details of any resulting actions taken are published on the Virtual Learning Environment and the Student Portal.

Additionally, on completion of their programme of study students will be invited to take a survey that seeks to measure what they have gained from their studies.

There are also opportunities for students to get involved in governance. An undergraduate and postgraduate student member is appointed by the University to the majority of committees through an annual appointment round. Some programmes also recruit student members at the programme level. Students are frequently invited to take part in quality review processes such as Periodic Programme Reviews, Programme approval, Thematic Reviews, MOOC review panels and ad hoc focus groups. Opportunities such as these are advertised through social media and on the website. More information can be found on the website.

Students can also apply to join the Student Voice Group, which meets four times a year to consider initiatives for enhancing student experience. Notes from these meetings are published on the Student Portal.

After graduation

Further study

Successful completion of the programme can allow students to progress to a higher level qualification in both the subject area and potentially many other subject areas. Enquiries about further study opportunities should be directed to the University of London Student Advice Centre '*ask a question'* button in the student portal.

Graduate employment routes

The programmes are designed to introduce the technical, legal and commercial aspects of cyber security. Graduates of these programmes will have a sound basis for a professional career as experts in cyber security, in both industry and commerce, and will go on to a range of different graduate employment routes. Successful completion of the MSc may allow students to progress to postgraduate research in the degree field.

The Alumni community

Upon graduation, students automatically become members of the University of London Alumni Network, a diverse community of over 100,000 alumni in more than 180 countries. The Alumni Network can provide individuals with lifelong links to the University of London and each other. Benefits include social and networking events, access to local groups, a bi-annual magazine, social networking groups, and the opportunity to become an Alumni Ambassador for the University of London.

Follow the alumni community on social media: Facebook, Instagram, LinkedIn

Appendix A – Structure of the programmes

A detailed outline of the module syllabus is provided on the Programme page, under structure

MSc Cyber Security

For the qualification of MSc Cyber Security you must pass

- The following core modules (each worth 15 credits):
  - CYM010 Cyber security foundations
  - CYM020 Security management and governance
  - CYM030 Cybercrime
  - CYM040 Applied cryptography
  - CYM050 Network and infrastructure security
  - CYM060 Computer systems security
  - CYM070 Software and application security
  - CYM080 Security and behaviour change
  - CYM090 Information privacy
  - CYM100 Research methods for cyber security
- One compulsory Project module (worth 30 credits):
  - CYM500 Project

PGDip Cyber Security

For the qualification of PGDip Cyber Security you must pass

- **One** core module (worth 15 credits):
  - CYM010 Cyber security foundations
- Any **seven** modules chosen from (each worth 15 credits):
  - CYM020 Security management and governance
  - CYM030 Cybercrime
  - CYM040 Applied cryptography
  - CYM050 Network and infrastructure security
  - CYM060 Computer systems security
  - CYM070 Software and application security
  - CYM080 Security and behaviour change

- CYM90 Information privacy

PGCert Cyber Security

For the qualification of PGCert Cyber Security you must pass

- **One** core module (worth 15 credits):
  - CYM010 Cyber security foundations
- Any **three** optional modules chosen from (each worth 15 credits):
  - CYM020 Security management and governance
  - CYM030 Cybercrime
  - CYM040 Applied cryptography
  - CYM050 Network and infrastructure security
  - CYM060 Computer systems security
  - CYM070 Software and application security
  - CYM080 Security and behaviour change
  - CYM090 Information privacy

Appendix B – Module descriptions

Cyber security foundations [CYM010]

This preliminary module, which must be taken before any of the other modules in the degree programme, introduces the broad range of concepts, challenges and technologies that underpin the provision of cyber security. Students will gain an understanding of what cyber security is, why it is important, and of the principal techniques and technologies that are used to achieve cyber security.

Gaining an understanding of certain key elements of cyber security is necessary to be able to properly appreciate individual aspects of the subject in greater detail. This module is intended to give students this broad understanding so that they can set the ideas and skills developed in other modules into a broader context.

Assessment: One online examination (100%)

Security management and governance [CYM020]

This module aims to generate understanding and appreciation of the need for effective security management and the main currently used approaches to management in practice, including key standardised approaches and the fundamental importance of a risk-based approach. After completing the module, students will also understand key components of practical cyber security management, including the impact of law and regulation, the importance of auditing, and the key role of people in achieving cyber security. To help students understand the importance of effective security management, case studies of failures will be considered.

This module plays a fundamental role in binding together all the other modules of the degree programme; it will address the issue of how to integrate the wide range of possible technologies and techniques for information security into a real-world Information Security Management System for an organisation.

Assessment: One online examination (100%)

Cybercrime [CYM030]

Cybercrime is a complex topic which affects individuals, societies and nations. There is an increasing manifestation of various types of cybercrime, which are either new or evolving. In order to understand the cybercrime environment, this module synthesises its dynamically changing economic, technical, political and psychological components. We explore the types of cybercrime, their manifestations, and their underlying mechanisms. Legal measures and challenges are explored, in view of the global nature of cybercrime. The evolution and the trends of cybercrime are analysed along various models adopted by criminals. Students will gain an understanding of the tools and approaches used in digital forensics and analyse real-world cases of cybercrime.

Assessment: One online examination (100%)

Applied cryptography [CYM040]

Cryptography provides the core toolkit that underpins most digital security technologies. An understanding of what cryptography does, and its limitations, is critical to developing a wider appreciation of the security of everyday digital applications. Since cryptography provides tools for atomic security services such as confidentiality and data integrity, an appreciation of cryptography also equips students with a fundamental understanding of what security means

in cyberspace. Note that this module adopts a non-mathematical approach to cryptography, very much considering it from the perspective of what any good cyber security professional needs to know, and avoiding unnecessary technical details.

In this module students will explore the role of cryptography in supporting digital security for everyday applications such as the internet, mobile phones, wireless networks and cryptocurrency. Students will develop an understanding of the functionality and purpose of the main cryptographic tools we use today. Students will learn how to make decisions about which cryptographic tools are most appropriate to deploy in specific settings. Students will also explore the wider infrastructure surrounding cryptography and how this impacts the overall security of systems deploying cryptography.

Assessment: One online examination (100%)

Network and infrastructure security [CYM050]

Computer networking technologies and cyber-physical systems form the infrastructure of organisations and businesses, the internet and the web-based application ecosystem as well as critical national infrastructure. This module provides the foundations for us to understand the design and security of an organisations network, operational technologies, the internet and critical infrastructure. Computer networking provides the foundational connectivity services that are used for the world wide web, distributed computer applications and services, operations and manufacturing, and national infrastructure.

This module discusses vulnerabilities and the exploits that target computer networks and systems, the internet infrastructure and provides an introduction to modelling, assessing and testing networks and systems. Key aspects are explored through case studies and we complement the Computer systems security and the Software and application security modules.

Assessment: One online examination (100%)

Computer systems security [CYM060]

Computer systems form the infrastructure of organisations, the internet and the web-based application ecosystem. This module provides the foundations for us to understand the computer systems from the operating systems and security services. The module allows us to consider case studies from a wide range of deployments including the internet and cloud computing/infrastructure that provide the world wide web and distributed computing services.

Assessment: One online examination (100%)

Software and application security [CYM070]

Software and applications form the key business functionality in organisations. Building secure software is critical to the business and must be considered alongside secure computer systems and networks/infrastructure.

This module introduces the principles around software and applications, including security and the issues of malicious software. The module outlines techniques used for secure software development, principles of secure programming, most common software vulnerabilities that can be introduced during software development and concludes with discussion of the wider considerations and research direction for software and application security. Key aspects are explored through a number of topical case studies, such as web

and cloud and this module complements the Computer systems security and Network and infrastructure security modules.

Assessment: One online examination (100%)

Security and behaviour and change [CYM080]

Security is heavily dependent on humans and their actions. These actions can either strengthen or diminish security levels. In this module students are introduced to the relationships between security and human behaviour, in multiple settings. We consider perceptions and practical implementations of security, on both individual and group/societal level. We utilise concepts from behavioural economics, decision-making and psychology, along with mechanisms to design and encourage changes in security behaviours. Finally, we examine the construct of a security culture and its relationships with norms, habits and awareness training.

Assessment: One online examination (100%)

Information privacy [CYM090]

This module will introduce students to the challenges facing any organisation in managing data privacy. Students will gain an understanding of the meaning of data privacy, and will examine the serious legal constraints facing all organisations which make data privacy a key issue for cyber security risk management. Students will examine key governance matters, including privacy impact assessments, and the role of technology in supporting privacy will also be considered, including de-identification techniques for datasets, homomorphic encryption, and other privacy enhancing technologies. Finally, a privacy case study, such as e-voting, will be described.

Assessment: One online examination (100%)

Research methods for cyber security [CYM100]

This module provides students with an introduction to research methods in cyber security such that they can choose and investigate a research or professional topic for their project. The project topic can be from across the CyBOK Knowledge Areas and professional frameworks such as the CIIsec Knowledge and Skills frameworks. The output from the module is a report that describes the project, provides an initial literature review and a project plan.

Assessment: Project description and plan (100%)

Project [CYM500]

This module provides the student an opportunity to undertake an individual dissertation project in the discipline of cyber security. A project is a major individual piece of work. It can be of academic or professional nature and aimed at acquiring and demonstrating understanding and the ability to reason about some specific area of cyber/information security. The project may be academic in nature or document the ability of organisations or individuals to deal with a practical aspect of cyber/information security. The project represents the key difference between the Postgraduate Diploma, which is a taught qualification, and the award of an MSc which incorporates this substantial piece of individual work.

Assessment: One research project (100%)