



U
F
ER
D
Y

Programme Regulations 2022–2023

Information Security

MSc
PGDip
Individual modules

Important document – please read
This document contains important information that governs our registration, assessment and programme of study

Important information regarding the Programme Regulations	2
Alternative assessments during the Coronavirus (COVID-19) outbreak.....	3
1 Structure	4
2 Programme redevelopment and withdrawal.....	5
3 Registration	5
4 Recognition of prior learning and credit transfer	5
5 Module selection.....	6
6 Assessment for the programme	7
7 Retaking an assessment	9
8 Progression within the programme.....	11
9 Schemes of award.....	13
Appendix A Structure of the programmes	16
Postgraduate Diploma in Information Security	16
MSc in Information Security.....	17
Appendix B Module outlines	18
Core element	

Important information regarding the Programme Regulations

About this document

Last revised 29 March 2022

As a student registered with the University of London you are governed by the current General Regulations and Programme Regulations associated with your programme of study.

The Programme Regulations are designed and developed by Royal Holloway, University of London, which is responsible for the

Alternative assessments during the Coronavirus (COVID-19) outbreak

In line with our current General Regulations, the University may offer you alternative assessments during the COVID-19 outbreak.

1 Structure

[Appendix B](#) gives the module outlines.

Qualifications

1.1

The following named qualifications are awarded

1.7

We may decide that you must successfully complete either one or two modules on a stand-alone basis before we will consider your application to register for the PGDip or MSc Information Security.

2 Programme redevelopment and withdrawal

2.1

It is no longer possible to register for the Information Security programme.

3 Registration

Effective date of registration

3.1

For any queries regarding recognition and accreditation of prior learning, contact us using the

6 Assessment for the programme

In line with our current General Regulations, the University may offer you alternative assessments where necessary. This includes holding online timed assessments in place of

6.16

You must submit an electronic version of the completed dissertation to arrive not later than 31 March (BST) in the academic year of submission. The electronic submission is via the VLE unless otherwise agreed. In the case of an interruption of the Project the dissertation should normally be submitted in the following year.

7 Retaking an assessment

Maximum number of attempts

7.1

The maximum number of attempts permitted at any element of assessment for a module is two.

7.6

If you receive the result of 'Fail' on your second attempt at the assessment for a module, and you are still eligible to progress, then the highest mark for that module may be carried forward and considered for classification. However if you are no longer able to satisfy the requirements for the PGDip or MSc degree then your registration will cease and the Board of Examiners will consider whether you are eligible for an exit qualification.

Mark used for classification

7.

7.13

If you retake the Project module you have the following options:

to keep the same Project topic and make another attempt with no further supervision, normally recommended for students who receive a mark of 40-49% on their first attempt at the project report

to keep the same Project topic (or a related topic) and make another attempt with reduced supervision

to start again with a new Project topic and full supervision.

7.14

If you submit a Project dissertation report you will be considered to have made an attempt at the Project.

If registered for an Individual module

7.15

If you are registered for an individual module and you receive the result of 'Fail' on your second attempt at the assessment for the module, then the highest mark for that module will count as the final result. If you apply to progress to the related PGDip or degree and this is approved, this mark will be taken into account for classification purposes.

8 Progression within the programme

See [Section 6](#) for method of assessment.

8.1

In any eoEctθ

Transfer from the MSc Information Security to the PGDip Information Security

8.5

If you are registered for the MSc Information Security you may transfer to the PGDip at any time providing you are able to satisfy the conditions for that award.

Transfer from Individual modules

8.6

A mark or grade awarded for completion of an individual module may not be used to replace any mark or grade for a degree or diploma already awarded.

8.7

We will consider the transfer from an individual module to the PGDip or MSc on a case-by-case basis upon receiving a request to this effect.

You can request to transfer from an individual module to the PGDip or MSc by logging an enquiry via the *ask a question* button in the [Student Portal](#).

Previous study recommended for Options modules

8.8

Students with relevant professional experience are not required to have completed the following previous study before taking Options

9.7

The PGDip may be awarded if a student achieves an overall weighted average of at least 50%, with no mark in any taught module which counts towards the final assessment falling below 50%. Failure marks between 40–49% are not usually condoned for the award of a PGDip, but if they are, such condoned fails would be in modules which do not constitute more than 40 credits.

9.8

To be considered for an award with *distinction* for the PGDip Information Security, you must have obtained an overall average of at least 70%.

9.9

To be considered for an award with *merit* for the PGDip Information Security, you must have obtained an overall average of at least 60%.

9.10

A candidate for the award of the PGDip who satisfies both the following criteria will automatically be raised into the next class of award:

- (a) the overall weighted average mark must fall within 2% of one of the classification boundaries in paragraphs 8.7, 8.8 and 8.9, and
- (b) the mark for at least 60 credits counting towards the award is above the classification boundary. The dissertation may be included in these 60 credits.

PGDip Information Security credits.

9.15

The Board of Examiners will decide if you can be awarded the PGCert Information Security. The Board of Examiners must be satisfied that the qualification represents a coherent programme of study.

9.16

To be considered for an award with distinction for the PGCert Information Security, you must have obtained an overall average of at least 70%.

9.17

To be considered for an award with merit for the PGCert 595.32 841.92 reW*nBTith merit for the

Appendix B Module outlines

Core element

Security management [IYM001]

Aims

This module will emphasise the need for good security management. Its aims are to identify the problems associated with security management and to show how various (major) organisations solve those problems.

Objectives

On completion of the module, the student will appreciate the complexities of security management, and have seen how some companies attempt to solve these problems.

Assessment

One two-hour unseen written paper.

An

Objectives

At the end of the module students should have gained an understanding of the fundamentals of the provision of security in information networks, as well as an appreciation of some of the problems that arise in devising practical solutions to network security requirements.

Assessment

One two-hour unseen written paper.

Computer security [IYM004]

Aims

This module deals with the more technical means of making a computing system secure. This process starts with defining the proper security requirements, which are usually stated as a security policy. Security models formalise those policies and may serve as a reference to check the

Objectives

On completion of the module the students should be able to:

- recognise a variety of security issues that arise in applications;
- review how the various security issues in a particular application relate to one another;
- understand how and why businesses address specific security concerns in their applications;
- appreciate the various aspects of integrating security into the application development lifecycle;
- analyse how security aims are met in a particular application;
- evaluate the effectiveness of security mechanisms in the technical and business context of the case studies.

Assessment

Objectives

On completion of the module students should be able to:

- follow trends in cyber crime;
- relate cyber security methodologies to criminal methods;
- detect criminal activity in a computerised environment;
- apply the criminal and civil law to cyber criminality;
- understand how viruses, logic bombs and hacking are used by criminals;



Identity personality traits that affects individual security behaviours.

Carry out privacy impact assessments, develop privacy policies and implement the appropriate privacy preserving controls.

Develop, implement security awareness programs.

Assessment

One two hour unseen written paper.

Project element

Project [IYM011]

Aims

The Project is a major individual piece of work. It can be of academic nature and aimed at acquiring and demonstrating understanding and the ability to reason about some specific area of information security. Alternatively, the Project work may document the ability to deal with a practical aspect of information security.

Objectives

The student will write a comprehensive dissertation on an information security topic. On completion of the Project students should have demonstrated their ability to:

work independently on a security-related project, for which they have defined the objectives and rationale;

apply knowledge about aspects of information security to a particular problem, which may be of an engineering, analytical or academic nature;

Appendix C Assessment criteria

Where examinations feature essay-style questions, the following grade description criteria apply:

%	No specific marks are awarded for spelling, punctuation or grammar. However, any significant weaknesses in these areas which result in the examiner having difficulty comprehending an answer may result in less credit being awarded.
85+	Outstanding levels of accuracy and technical competence; deep understanding; near-comprehensive knowledge; exceptional independence of thought; exceptionally well-organised and original answers; high levels of ability in analysis of information; coherent structure; completely addresses all aspects of the question. As good as could be expected under examination conditions.
70-84	Very high levels of accuracy and technical competence; deep understanding; detailed knowledge; may show some originality in interpretation or analysis; high degree of creativity and independence of thought; high levels of ability in the analysis of quantitative or qualitative information; coherent structure; completely addresses all aspects of the question.
60-69	Good degree of accuracy and technical competence; clear understanding; good breadth of knowledge; some evidence of creativity and independence of thought; generally effective analysis of quantitative or qualitative information; coherent structure; arguments are well constructed; addresses most key aspects of the question.
50-59	

