SCHOOL OF ENGINEERING, PHYSICAL AND MATHEMATICAL SCIENCES

DEPARTMENT OF INFORMATION SECURITY

POSTGRADUATE TAUGHT STUDENT HANDBOOK

2020/2021
Department of Information Security  
School of Engineering, Physical and Mathematical Sciences  
Bedford Building  
Royal Holloway, University of London  
Egham Hill, Egham  
Surrey, TW20 0EX

Telephone +44 (0)1784 276881  
Email EPMS-School@rhul.ac.uk

Disclaimer

This document was published in September 2020 and was correct at that time. The department* reserves the right to modify any statement if necessary, make variations to the content or methods of delivery of courses of study, to discontinue courses, or merge or combine courses if such actions are reasonably considered to be necessary by the College. Every effort will be made to keep disruption to a minimum, and to give as much notice as possible.

* Please note, the term ‘department’ is used to refer to ‘departments’, ‘Centres and Schools’. Students on joint or combined degree courses should check both departmental handbooks.
Contents

1 INTRODUCTION TO YOUR DEPARTMENT ................................................................. 5
1.1 WELCOME ........................................................................................................... 5
1.2 HOW TO FIND US: THE DEPARTMENT ............................................................ 5
1.3 MAP OF THE EGHAM CAMPUS ....................................................................... 6
1.4 HOW TO FIND US: THE STAFF ....................................................................... 7
1.5 HOW TO FIND US: THE SCHOOL OFFICE ....................................................... 9
1.6 THE DEPARTMENT: PRACTICAL INFORMATION ............................................. 9
1.7 STAFF RESEARCH INTERESTS ........................................................................ 9

2 SUPPORT AND ADVICE ....................................................................................... 9
2.1 SUPPORT WITHIN YOUR SCHOOL ................................................................. 9

3 COMMUNICATION .............................................................................................. 10
3.1 POST ................................................................................................................. 10
3.2 NOTICE BOARDS ............................................................................................ 10
3.3 PERSONAL TUTORS ....................................................................................... 10
3.4 QUESTIONNAIRES .......................................................................................... 10

4 TEACHING........................................................................................................... 11
4.1 DATES OF TERMS ............................................................................................ 11
4.2 LECTURES ........................................................................................................ 11
4.3 TUTORIALS, WORKGROUPS AND OFFICE HOURS ....................................... 11
4.4 WORKSHEETS ............................................................................................... 12
4.5 TEXTBOOKS AND THE WEB ......................................................................... 12

5 DEGREE STRUCTURE ......................................................................................... 12
5.1 DEPARTMENT SPECIFIC INFORMATION ABOUT DEGREE STRUCTURE ........ 12
5.2 THE THREE ELEMENTS .................................................................................. 13
5.2.1 Core Element ............................................................................................. 13
5.2.2 Options Element ....................................................................................... 14
5.2.3 Pathways ................................................................................................... 14
5.2.4 Project Element ....................................................................................... 14
5.3 PROGRAMME SCHEDULE ............................................................................ 15
5.4 COURSE REGISTRATIONS ............................................................................. 15
5.5 CHANGE OF COURSE .................................................................................... 16

6 FACILITIES ....................................................................................................... 16
6.1 FACILITIES AND RESOURCES WITHIN YOUR DEPARTMENT ................... 16
6.2 THE LIBRARY .................................................................................................. 16
6.3 PHOTOCOPIING AND PRINTING .................................................................. 16
6.4 COMPUTING ................................................................................................... 16
6.4.1 IT Helpdesk and Support ......................................................................... 16
6.4.2 Acceptable Use Policy ............................................................................. 17

7 DISSERTATION .................................................................................................. 17
7.1 THE DISSERTATION ......................................................................................... 17
7.2 CHOICE OF DISSERTATION TOPIC .............................................................. 17
7.3 THE DISSERTATION SUPERVISOR .................................................................. 17
7.4 CONTENT OF DISSERTATION ....................................................................... 17
7.5 PROGRESSION TO THE DISSERTATION ...................................................... 18

8 ASSESSMENT INFORMATION ............................................................................ 18
8.1 ANONYMOUS MARKING AND COVER SHEETS ........................................ 18
8.2 SUBMISSION OF WORK ................................................................................. 18
1 Introduction to your department

1.1 Welcome

Welcome to Royal Holloway. Royal Holloway, University of London (hereafter ‘the College’) is one of the UK’s leading research-intensive universities, with six academic schools spanning the arts and humanities, social sciences and sciences.

Welcome to the Information Security Group. This booklet is prepared for students that registered for the Information Security Group’s MSc degree programme in Information Security. The aim of the booklet is to provide students with essential information on:

1. College policies and facilities
2. The Information Security Group (ISG)
3. Academic and pastoral support arrangements
4. Departmental quality assurance procedures
5. Procedures for complaints and academic appeals
6. Coursework, study and revision advice.

1.2 How to find us: the Department

Information Security is located in the Bedford Building.
Please note, student parking is very limited and is not available if you live in Halls or within 1.5 miles of campus. If you do live more than 1.5 miles away or have a particular reason why you need to come to campus by car, you must apply for a parking permit. If you have a motorbike or scooter you must also register the vehicle with College. Find more information about the Parking Permit portal here.
1.4 How to find us: the staff

**CONTACT DETAILS**

**Head of School:** Professor Stewart Boogert  
Room Bedford 1-27  
Telephone 01784 414062  
Email steward.boogert@rhul.ac.uk

**Head of Department:** Professor Peter Komisarczuk  
Room Bedford 1-13  
Telephone 01784 443089  
Email peter.komisarczuk@rhul.ac.uk

**School Manager:** Vanessa Law  
Room Bedford 1-28  
Telephone 01784 443598  
Email Vanessa.Law@rhul.ac.uk

**School Helpdesk:** Carole Pearce  
Room Bedford 1-29  
Telephone 01784 276881  
Email EPMS-School@rhul.ac.uk

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Room</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professor Martin Albrecht</td>
<td>01784 414922</td>
<td>Bedford 2-03</td>
<td><a href="mailto:martin.albrecht@rhul.ac.uk">martin.albrecht@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Chair of Information Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dr Jorge Blasco Alis</td>
<td>01784 443116</td>
<td>Bedford 1-24</td>
<td><a href="mailto:Jorge.BlascoAlis@rhul.ac.uk">Jorge.BlascoAlis@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Course Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professor Carlos Cid</td>
<td>01784 414685</td>
<td>Bedford 2-02</td>
<td><a href="mailto:carlos.cid@rhul.ac.uk">carlos.cid@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Chez Ciechanowicz</td>
<td>0178444 3112</td>
<td>Bedford 1-10</td>
<td><a href="mailto:z.ciechanowicz@rhul.ac.uk">z.ciechanowicz@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Lizzie Coles-Kemp</td>
<td>0178444 3084</td>
<td>Bedford 2-05</td>
<td><a href="mailto:lizzie.coles-kemp@rhul.ac.uk">lizzie.coles-kemp@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor of Information Security: RI Lead</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professor Jason Crampton</td>
<td>0178444 3117</td>
<td>Bedford 1-10</td>
<td><a href="mailto:jason.crampton@rhul.ac.uk">jason.crampton@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Director of Research</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dr Salaheddin Darwish</td>
<td>0178427 6940</td>
<td>Bedford 1-08</td>
<td><a href="mailto:salaheddin.darwish@rhul.ac.uk">salaheddin.darwish@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Jassim Happa</td>
<td>01784 276863</td>
<td>Bedford 1-14</td>
<td><a href="mailto:jassim.happa@rhul.ac.uk">jassim.happa@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Darren Hurley-Smith</td>
<td>TBC</td>
<td>Bedford 1-03</td>
<td><a href="mailto:Darren.Hurley-Smith@rhul.ac.uk">Darren.Hurley-Smith@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Rikke Jensen</td>
<td>0178427 6549</td>
<td>Bedford 2-04</td>
<td><a href="mailto:rikke.jensen@rhul.ac.uk">rikke.jensen@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Kostas Markantonakis</td>
<td>0178441 4409</td>
<td>Bedford 1-04</td>
<td><a href="mailto:k.markantonakis@rhul.ac.uk">k.markantonakis@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Smart Card Centre Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professor Keith Martin</td>
<td>0178444 3099</td>
<td>Bedford 1-12</td>
<td><a href="mailto:keith.martin@rhul.ac.uk">keith.martin@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Director CDT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professor Keith Mayes</td>
<td>0178441 4408</td>
<td>Bedford 1-05</td>
<td><a href="mailto:keith.mayes@rhul.ac.uk">keith.mayes@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Name</td>
<td>Phone</td>
<td>Bedroom</td>
<td>Email</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Dr Konstantinos Mersinas</td>
<td>0178444 3079</td>
<td>1-15</td>
<td><a href="mailto:Konstantinos.Mersinas@rhul.ac.uk">Konstantinos.Mersinas@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Chris Mitchell</td>
<td>0178444 3423</td>
<td>2-17</td>
<td><a href="mailto:c.mitchell@rhul.ac.uk">c.mitchell@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Sean Murphy</td>
<td>0178444 3699</td>
<td>2-01</td>
<td><a href="mailto:s.murphy@rhul.ac.uk">s.murphy@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Siaw-Lynn Ng</td>
<td>0178441 4397</td>
<td>2-30</td>
<td><a href="mailto:s.ng@rhul.ac.uk">s.ng@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Rachel Player</td>
<td>TBC</td>
<td>1-06</td>
<td><a href="mailto:Rachel.player@rhul.ac.uk">Rachel.player@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Dr Geraint Price</td>
<td>0178441 4160</td>
<td>1-09</td>
<td><a href="mailto:geraint.price@rhul.ac.uk">geraint.price@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Carlos Cid</td>
<td>0178427 6305</td>
<td>2-06</td>
<td><a href="mailto:Carlos.cid@rhul.ac.uk">Carlos.cid@rhul.ac.uk</a></td>
</tr>
<tr>
<td>MSc Project Coordinator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dr Daniele Sgandurra</td>
<td>0178441 4423</td>
<td>1-23</td>
<td><a href="mailto:daniele.sgandurra@rhul.ac.uk">daniele.sgandurra@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Stephen Wolthusen</td>
<td>0178444 3270</td>
<td>2-31</td>
<td><a href="mailto:stephen.wolthusen@rhul.ac.uk">stephen.wolthusen@rhul.ac.uk</a></td>
</tr>
</tbody>
</table>

**Visiting Professors:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professor Henry Beker</td>
<td></td>
</tr>
<tr>
<td>Professor Andy Clark</td>
<td><a href="mailto:andy.clark@rhul.ac.uk">andy.clark@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Whitfield Diffie</td>
<td></td>
</tr>
<tr>
<td>Professor Paul Dorey</td>
<td><a href="mailto:paul.dorey@csoconfidential.com">paul.dorey@csoconfidential.com</a></td>
</tr>
<tr>
<td>Professor Dieter Gollmann</td>
<td></td>
</tr>
<tr>
<td>Professor Igor Muttik</td>
<td></td>
</tr>
<tr>
<td>Professor David Naccache</td>
<td><a href="mailto:david.naccache@rhul.ac.uk">david.naccache@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Professor Richard Walton</td>
<td><a href="mailto:richard.walton@rhul.ac.uk">richard.walton@rhul.ac.uk</a></td>
</tr>
</tbody>
</table>

**Consultants:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professor Fred Piper</td>
<td><a href="mailto:f.piper@rhul.ac.uk">f.piper@rhul.ac.uk</a></td>
</tr>
<tr>
<td>External Relations Director</td>
<td></td>
</tr>
</tbody>
</table>

**Senior Visiting Fellows:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Carolina</td>
<td><a href="mailto:robert.carolina@rhul.ac.uk">robert.carolina@rhul.ac.uk</a></td>
</tr>
</tbody>
</table>
### Technical Staff:

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Room</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Francesco Fildani</td>
<td>01784 443315</td>
<td>Bedford 0-02</td>
<td><a href="mailto:francesco.fildani@rhul.ac.uk">francesco.fildani@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Claire Matthews</td>
<td>01784 276095</td>
<td>Bedford 0-02</td>
<td><a href="mailto:claire.matthews@rhul.ac.uk">claire.matthews@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Narinderpal Sehra</td>
<td>01784 443111</td>
<td>Bedford 0-02</td>
<td><a href="mailto:narinderpal.sehra@rhul.ac.uk">narinderpal.sehra@rhul.ac.uk</a></td>
</tr>
<tr>
<td>Adrian Thomas</td>
<td>01784 443428</td>
<td>Bedford 0-02</td>
<td><a href="mailto:adrian.thomas@rhul.ac.uk">adrian.thomas@rhul.ac.uk</a></td>
</tr>
</tbody>
</table>

1.5 **How to find us: the School office**

The ISG – that is, the staff and administrative offices is located in the Bedford Building.

1.6 **The Department: practical information**

The Information Security Group has social media groups aimed at anyone who wants to keep up to date with their activities. We use them to communicate news from the department and we hope that they will allow students and faculty members to keep in contact with each other after graduation. We currently have social media pages on Linked In, Facebook, Twitter and YouTube:

- **Twitter:** [https://twitter.com/ISGnews](https://twitter.com/ISGnews)
- **Facebook:** [https://www.facebook.com/ISGofficial](https://www.facebook.com/ISGofficial)
- **LinkedIn:** [https://www.linkedin.com/groups/3859497](https://www.linkedin.com/groups/3859497)
- **YouTube:** [https://www.youtube.com/channel/UCKUK0JK5pjVAL3qop-lUdKA](https://www.youtube.com/channel/UCKUK0JK5pjVAL3qop-lUdKA)

Further information can be found on the Information Security website via the Student Intranet pages.

1.7 **Staff research interests**

In the UK Research Assessment Exercise (the REF) 2014, 99% of the department’s research publications and conference papers were rated as of international quality, with over a third recognised as world leading, and a further half internationally excellent. Our research feeds into Unit of Assessment 11 (Computer Science), Unit of Assessment 10 (Mathematics) and the ISG will also be contributing to Unit of Assessment 12 (Engineering) in the REF 2021. The research interests of individual ISG staff can be found in the Staff Directory section of the ISG website – [https://www.royalholloway.ac.uk/isg/home.aspx](https://www.royalholloway.ac.uk/isg/home.aspx) and show a wide range of research expertise across the disciplines that make up information security.

2 **Support and advice**

2.1 **Support within your School**

The School Helpdesk is there to help you with any questions or concerns you might have about your studies. Opening hours are 9:00am to 5:00pm in term time and 10:00am to 4:00pm during vacation. The Helpdesk is staffed throughout these opening hours. You can ring 01784 276881 during office hours or email EPMS-School@rhul.ac.uk.
Depending on your query, the Helpdesk will answer your questions, book you an appointment, put you in touch with a colleague who can help, or refer you another professional team within the College. The Helpdesk is situated in room 1-29, in Bedford Building.

To book an appointment

Most queries can be managed via email, phone or MSTeams but should you need a face to face appointment the office team will book a 15 minute appointment with you. To arrange a face to face meeting email EPMS-School@rhul.ac.uk providing your student ID and a brief explanation of what you want to discuss during the appointment.

3 Communication

3.1 Post

Students should not use the College address for private mail.

Administrative staff will alert you by email of any internal mail received by the Department/School.

3.2 Notice boards

Notices related to your course will be posted on Moodle or will be sent to your student email account.

It is your responsibility to check the times and venues of all class meetings and of any requirements (e.g. essay deadlines) relating to your courses, so, if in doubt, please ask!

3.3 Personal Tutors

The academic and pastoral welfare of MSc students is conducted through the personal tutors. Lists allocating students to tutors will be circulated through the normal channels (i.e. email) at the beginning of the Academic Year.

Each student is assigned a member of staff to act as personal tutor. The role of the tutor is to guide the advisee’s academic progress (particularly during the initial phase of the MSc Project) and provide pastoral care for the advisee throughout the duration of the programme of study. Students can discuss any academic, financial, medical or other problems with their tutor as soon as they arise. The tutor may then be able to recommend an appropriate source of help, and be able to act on the student’s behalf. Any personal information you impart will be treated in strict confidence.

Students should establish initial contact with their tutor at the beginning of the Autumn term

3.4 Questionnaires

Course questionnaires, issued at the end of each course are used as a means of assessing student views. These are augmented by a final end of year questionnaire in which students are asked to comment in general about the whole MSc (with the benefit of having completed all elements of the programme). These form an essential part of our procedures to monitor the quality of our provision and they are invaluable in course planning and improvement. For the system to work it is imperative that we have a high percentage of returns and that the questionnaires have been filled in thoughtfully. For each taught course the completed anonymous questionnaires are scanned by an outside contractor, and the summaries are presented to the Student-Staff Committee and to all staff. The comments on the back of the questionnaires are passed to the appropriate lecturers, to the Head of Department and to the MSc Programme Director.
4 Teaching

4.1 Dates of terms

Term dates for the year are as follows.

**Autumn term:** Monday 21 September to Friday 11 December 2020
**Spring term:** Monday 11 January to Friday 26 March 2021
**Summer term:** Monday 26 April to Friday 11 June 2021

4.2 Lectures

Students in the Information Security Group are expected to attend all lectures. This year, we have implemented a set of measures to mitigate the risks generated by the ongoing pandemic.

The method of instruction will vary for each of the courses. For each of them, there will normally be a time-tabled session that you will be able to attend face to face. In order to adhere with social distancing requirements this session may be split in two groups. You will be informed of this in advance via Moodle. Some of these sessions may have to run fully online due to self-isolation requirements required for staff members. Students that cannot attend campus sessions due to self-isolation requirements will also be able to follow these online. Additional learning materials will be provided online in the form of pre-recorded videos, activities, etc. Students are also expected to read and engage with the additional materials in order to complement the material delivered during formal lectures.

In addition to the above, a subset of the MSc courses is also delivered through “block mode”. Part-time students that make use of this delivery mode are able to study a specific course during an intensive 5 day period. This year, autumn modules will have their block mode delivered in the spring term while spring term modules will be delivered in block mode during the summer term. The availability of these modules depends on the number of students who register for them.

Students are very much encouraged to ask questions during lectures. A considerable proportion of lectures are delivered by industry experts and their opinions are very much valued within the context of the MSc.

Please note there are no reading/study weeks for this PGT course.

4.3 Tutorials, Workgroups and Office Hours

Students are strongly encouraged to form informal workgroups which serve to promote cross-fertilisation between the very diverse range of students, some of whom already have a wealth of industrial/business/information security experience. There is no doubt that such workgroups have a very positive effect on students’ understanding of information security (and also a positive effect on exam results!).

All lecturers have office hours for dealing with students’ questions about the syllabus or the worksheets relating to given courses. These will be posted on Moodle and will normally be carried out via MS Teams.

Additional tutorials may also be available during the first term for any students needing to consolidate their background knowledge in particular areas such as basic maths for cryptography.
4.4 Worksheets
In most courses the lecturer will give out worksheets (via Moodle). All students are expected to attempt these worksheets. Depending on the lecturers’ preferences, some work may be marked and may be accompanied by model solutions. Students may also discuss their solutions with lecturers.

4.5 Textbooks and the Web
Although your lecture notes and worksheets form the key part of a course, you will need to consult other sources. At the start of each course the lecturer will tell you which books are most useful, and possibly suggest other less important texts. Throughout each course, lecturers will also point students in the direction of relevant web pages and other content. Please be cautious when using web resources since they may contain incorrect or misleading information.

We welcome comments about books in the library. If you think that more copies of an important textbook are needed in the library, or you find a book that you think should be there, tell the lecturer concerned. Remember, though, that it may take a little while for a book to be bought and appear on the shelves.

Eva Dann is the Information Consultant for Information Security, eva.dann@rhul.ac.uk

5 Degree structure
Full details about your course, including, amongst others, the aims, learning outcomes to be achieved on completion, modules which make up the course and any course-specific regulations are set out in the course specification available through the Course Specification Repository.

5.1 Department specific information about degree structure
The MSc in Information Security programme is offered by the Royal Holloway Information Security Group (ISG), which is an interdisciplinary research group including computer scientists, social scientists and mathematicians. It is one of the largest groups of academic security researchers in the world and all members of the group have strong links with external organisations involved with information security and secure digital business, including many of the largest such organisations in the country.

The programme provides students with a systematic understanding and critical awareness of current threats to the security of electronic information and the measures available to counteract these. To ensure that this Masters’ programme is at the forefront of developments in information security, several of the courses involve significant input from recognised security experts in industry and commerce. The programme will include study of a range of technologies such as cryptography, network security and computer security as well as considering the management of security, the commercial and regulatory issues and the many trade-offs and subjective issues that need to be addressed when implementing information security within an organisation. It will also develop the discipline-specific and transferable skills required for a professional career and for postgraduate research in information security.

The programme is normally studied full-time over one year (50 weeks), or normal part-time over two years (100 weeks). However it is possible to study the MSc over a period up to five years through CPD part-time (Continuing Professional Development Mode).
The aims of this Masters programme are to:

- provide advanced study of the technical, legal and commercial aspects of information security supported by research staff and recognised security experts from industry;
- examine critically current strategies, methodologies and techniques in information security;
- examine the main security issues in the development of digital business activities;
- develop a critical awareness of current problems in information security together with strategies and countermeasures for addressing these;
- relate the academic study of security to matters of public concern;
- develop the subject-specific and generic skills and techniques that will facilitate progression to MPhil/PhD studies in information security or a related field;
- develop the written presentation skills needed for the effective communication of security-related findings at advanced level;
- Foster the ability to learn independently, whether for career enhancement, progression to research, or personal intellectual development; provide a strong foundation for a professional career as a security expert in business or commerce.

5.2 The Three Elements

The MSc in Information Security has three main elements:
1. A core element made up of four core courses (four ninths of the total assessment)
2. An options element made up of two optional courses (two ninths of the total assessment)
3. A project element (three ninths of the total assessment)

The core element has two different forms, the selection of which depends on the interests and background of the student and their likely future career. Both forms of the core involve four taught courses.

Students may opt to also register for a Pathway (sometimes referred to as a track) which will limit their choices with respect to all three elements of the degree programme, i.e. the core, the options, and the project. Successful completion of an MSc pathway will indicate that the student has achieved a degree in a specialist sub-area within Information Security, and this will be acknowledged on the degree transcript.

5.2.1 Core Element

For the core element students must either follow Core A or Core B (but not both):

**Core A**

Students on Core A **must** take the following four courses (and are not allowed to take IY5522 or IY5523):

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5501</td>
<td>Security Management</td>
</tr>
<tr>
<td>IY5502</td>
<td>Introduction to Cryptography and Security Mechanisms</td>
</tr>
<tr>
<td>IY5511</td>
<td>Network Security</td>
</tr>
<tr>
<td>IY5512</td>
<td>Computer Security</td>
</tr>
</tbody>
</table>
Core B

Students on Core B must take the following four courses (and are not allowed to take IY5511 or IY5512):

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5501</td>
<td>Security Management</td>
</tr>
<tr>
<td>IY5502</td>
<td>Introduction to Cryptography and Security Mechanisms</td>
</tr>
<tr>
<td>IY5522</td>
<td>Security Technologies</td>
</tr>
<tr>
<td>IY5523</td>
<td>Secure Business Architectures</td>
</tr>
</tbody>
</table>

5.2.2 Options Element

Students must select two of the following courses:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5521</td>
<td>Legal and Regulatory Aspects of Electronic Commerce</td>
</tr>
<tr>
<td>IY5605</td>
<td>Cyber Crime</td>
</tr>
<tr>
<td>IY5606</td>
<td>Smart Cards, RFIDs and Embedded Systems Security</td>
</tr>
<tr>
<td>IY5607</td>
<td>Software Security</td>
</tr>
<tr>
<td>IY5609</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>IY5610</td>
<td>Security Testing Theory and Practice</td>
</tr>
<tr>
<td>IY5612</td>
<td>Cyber Security</td>
</tr>
<tr>
<td>IY5613</td>
<td>Human Aspects of Security and Privacy</td>
</tr>
</tbody>
</table>

5.2.3 Pathways

A student may optionally register for one of the following six pathways. These constrain the choices of the student in the following ways:

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Core</th>
<th>Mandatory Options</th>
<th>Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime</td>
<td>Core A</td>
<td>IY5605 and IY5609</td>
<td>Related to Cybercrime</td>
</tr>
<tr>
<td>Smart Cards, RFIDs and Embedded Systems Security</td>
<td>Core A</td>
<td>IY5606</td>
<td>Related to Smartcards, RFIDs or Embedded Systems</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>Core A or Core B</td>
<td>IY5612</td>
<td>Related to Cyber Security</td>
</tr>
<tr>
<td>Security Testing</td>
<td>Core A</td>
<td>IY5610</td>
<td>Related to Security Testing</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>Core A</td>
<td>IY5609</td>
<td>Related to Digital Forensics</td>
</tr>
<tr>
<td>Secure Digital Business</td>
<td>Core B</td>
<td>IY5521</td>
<td>Related to Secure Digital Business</td>
</tr>
</tbody>
</table>

5.2.4 Project Element

All students take the following compulsory element:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IY5500</td>
<td>Project</td>
</tr>
</tbody>
</table>
The **Project** is a significant piece of individual work of between 10,000 and 20,000 words. As a very rough guide the project report should be around 50 pages long. This measure assumes fairly dense text, reasonable line spacing, font size (typically between 10 and 12) and the use of reasonable margins.

**Project Submission Date:** With regard to dissertation submission, an electronic copy is required to be downloaded (date to be confirmed, but normally the 3rd week of August).

### 5.3 Programme Schedule

**Full-time students** take the four core courses in the Autumn term and two option courses in the Spring term followed by the independent project.

**Normal Part-time students** normally attend one day per week during term time. In the first year they take two of the four core courses in the Autumn term. The remaining core courses are taken in the Autumn term of the second year. Although not mandatory, we do recommend that all first year part-time students attend Security Management, together with Introduction to Cryptography and Security Mechanisms during the Autumn term. Students can take the options courses either in their first year or their second year or in both years. Students will normally do the independent project during their second year.

**CPD Part-time students** will spread their studies over a period of between three and five years.

**Exams** are always held during the third term (typically during the latter half of May). **We recommend that you immediately blank out this entire period in your diaries.** This is particularly important for part-time students who may have very significant work pressures.

### 5.4 Course Registrations

You can only register for 180 credits’ worth of courses in each academic year (this excludes courses which are being re-sat). You will have the option of changing courses up to the end of the second weeks after the start of teaching in each term (excluding Welcome week).

Full-time students are automatically registered for Security Management, Introduction to Cryptography, and the Project. The examinations office will, in due course provide students with information regarding exam registration. This will be augmented with extra information (from the ISG) that will be circulated via email.

Note that new normal part-time students can register for a certain number of options exams in their first year (up to a maximum of two). In their second year, part-time students can register for further options exams. However, the total number of options exams that can be sat (over two years) is restricted to two. A similar situation is true for CPD part-time students (the only difference is that the two year period is replaced with a period of up to five years).

While you have the option of changing course unit registrations within the first two weeks after the start of teaching (excluding Welcome Week) subject to agreement from the department, once you have submitted assessment for the course, you may not replace it with another either in that term or in a subsequent term (e.g. Spring term).
5.5 Change of course

Where provision is made for this in the programme specification, you may transfer to another programme, subject to the following conditions being met before the point of transfer:

(a) you must satisfy the normal conditions for admission to the new programme;
(b) you must satisfy the requirements in respect of mandatory courses and progression specified for each stage of the new programme up to the proposed point of entry;
(c) the transfer must be approved by both the department(s) responsible for teaching the new programme and that for which you are currently registered.
(d) if you are a student with Tier 4 sponsorship a transfer may not be permitted by Tier 4 Immigration rules.
(e) you may not attend a new programme of study until their transfer request has been approved.

Further information about changing programmes is available in Section 8 of the Postgraduate Taught Regulations.

You may apply to transfer from the Year-In-Industry programme to the standard MSc and vice versa.

6 Facilities

6.1 Facilities and resources within your department

Students in the Information Security MSc have access to Bedford building PC Labs – 0-04 and 0-06. Access to these labs is restricted to those times where there are no timetabled labs taking place. Access to these labs may also be restricted depending on social distancing and other pandemic-related restrictions. When using these labs it is imperative that all students follow the corresponding health and safety guidelines.

6.2 The Library

The Library is housed in the Emily Wilding Davison Building. The Information Consultant for Information Security is Eva Dann, who can be contacted at eva.dann@rhul.ac.uk

6.3 Photocopying and printing

The departmental printers and photocopier are reserved for staff use. Copier-printers (MFDs) for students are located in the Library, the Computer Centre and many PC labs, which will allow you to make copies in either black and white or colour.

6.4 Computing

How to find an available PC

6.4.1 IT Helpdesk and Support

ISG computer support may be obtained by logging a support ticket on CIMHelpDesk@rhul.ac.uk or by phone on (01784) 443 443.
6.4.2 Acceptable Use Policy

Use of ISG computer facilities and network infrastructure are covered by the ISG Acceptable Use Policy (AUP) in the final section of this document. You are required to accept the conditions of this policy before you are granted access to the ISG network and systems. You will be able to do this via Moodle. These conditions apply regardless of whether you are using your own laptop or an ISG system.

7 Dissertation

7.1 The Dissertation

This is a compulsory element that contributes three ninths to the total marks for the determination of the degree classification. A project is a major individual piece of work. It can be of academic nature and aim 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.

The student will write a comprehensive dissertation on the topic of the project. 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, and produce a well-structured report, including introduction, motivation, analysis, and appropriate references to existing work.

A detailed description of the project process and further information is available through the Moodle Project page (accessible to registered students). There are two project modules IY5500 and IY5510 (for year in industry students).

You should pay particular attention to the College policy on Penalties for late.

7.2 Choice of Dissertation Topic

More information about this can be accessed via the Moodle Project Page.

7.3 The Dissertation Supervisor

Your department will assign you a dissertation supervisor who will oversee your work. In most cases students are happy with the supervisory relationship. However, there are occasions where for some reason the supervisory relationship does not work and breaks down. If this happens, you should speak as soon as possible with your Personal Tutor and the Project Coordinator to see whether the problem can be resolved informally, e.g. through mediation, changing supervisor. You should not wait until after you have received your final degree results to raise the matter as it is very difficult for the College to resolve such matters or take remedial action at that point.

7.4 Content of Dissertation

The content and other requirements for the dissertation are covered by the MSc Project Handbook, available via Moodle.
7.5 Progression to the Dissertation

The decision on progression to the project is taken by the examination sub-board usually held near the end of June. Normally, to progress to the project a student must pass the taught part of the programme, i.e., achieve a pass mark (at least 50%) in every course or a mark of 40–49% in courses up to a total of 40 credits.

A student who did not pass the taught part of the programme may be allowed to progress to the project at the discretion of the sub-board. In order to graduate from the programme the student must then resit or repeat the failed courses in the next year according to the regulations.

8 Assessment information

8.1 Anonymous marking and cover sheets

All written exams are marked anonymously.

8.2 Submission of work

Details for submitting summative assignments will be circulated to students by course leaders. Assignments will be submitted via Moodle.

8.3 Progression to the Placement

For further details on Progression to the Placement, and the Placement, refer to the 'MSc in Information Security with Year in Industry Industrial Placement – Rules and Guidelines' which can be found on the IYMSC-202021 Moodle page.

For students on the year-in-industry programme, the decision on progression to the placement is taken by the examination sub-board. Please note that satisfying the progression requirements is not a guarantee that you will go on a placement; finding a placement remains the ultimate responsibility of the student. The main requirements for progression are as follows:

- Engage with the activities run by the Careers service throughout the year
- Achieve a good result in the January placement test
- Complete, submit and show good performance in all of the coursework assignments
- Exhibit exemplary attendance at all the lectures
- Engage with the project process during the Autumn and Spring term, and also submit a satisfactory Preliminary Literature Review by the required deadline (within the Spring Term)
- Pass each of the six taught courses
- Show competence in the use of English language within written assignments.

The decision on progression to the placement is taken by the Departmental Assessment Board usually held near the end of June.

A student on the year-in-industry programme who fails to satisfy the progression requirements or secure a placement is normally transferred to the corresponding programme not involving a placement. A student on a non-year-in-industry programme who wishes to transfer to the corresponding year-in-industry programme can qualify by fulfilling the progression requirements and finding a suitable placement.

All degree transfers are effected after the progression decision is made by the sub-board in June/July.
8.3.1 Preparation for placement
The Information Security Group and the College Careers Service run a number of activities throughout the year aimed at preparing students for a placement and helping them to secure a placement. In particular, during the Autumn term there are weekly Careers/Industry seminars and attendance at these is compulsory for all year-in-industry students. These seminars include sessions covering CVs and application forms.

All students on year-in-industry programmes should have their CV checked by the Careers Service. A first draft of the CV must be submitted to the Careers Service by the end of the Autumn Term. Failure to satisfy this requirement will lead to the student being asked to meet with the Course Director and a representative from the Careers Service. The Department may then remove the student from the year-in-industry programme.

8.3.2 Placement Test
One of the requirements for progressing to the placement is to pass the Placement Test. This test will be in the form of a written test that will examine in general terms what students have learned from studying the four core courses. Use of the English language and the ability to write in a clear structured manner will also contribute towards the assessment. The test will usually take place during the second or third week of the Spring term. Sample test questions will be provided beforehand.

8.3.3 Passing the examinations
Students who have passed the previous stages and have secured a placement with an employer are still required to pass the taught part of the programme in the Summer term exams (May) to actually go on the placement.

The final decision on a student’s progression to a placement is taken by the Departmental Assessment Board at the end of June/beginning of July. Students who have narrowly missed the required grades will be considered on an individual basis and may be allowed to progress at the discretion of the Departmental Assessment Board subject to good performance in the areas listed in the “Progression to the placement” subsection above. The placement therefore may not start before the Departmental Assessment Board meeting.

8.4 What to do if things go wrong – Extensions to deadlines
Please refer to the Extensions Policy and guidance on the College’s webpage about Applying for an Extension.

Please note: Not every assessment is eligible for an extension.

8.5 Support and exam access arrangements for students requiring support
Please see College handbook for details.

8.6 Academic misconduct - Plagiarism
Academic misconduct includes, but is not limited to plagiarism (see obelow), commissioning, duplication of work, (that is, submitting work for assessment which has already been submitted for assessment for the same or another course), falsification, impersonation, deception, collusion, (for example, group working would constitute collusion where the discipline or the method of assessment emphasises independent study and collective ideas are presented as uniquely those of the individual submitting the work), failure to comply with the rules governing assessment, including those set out in the ‘Instructions to candidates’.
The Regulations set out some of the types of academic misconduct in more detail, the procedures for investigation into allegations of such offences and the penalties. Students are strongly encouraged to read these Regulations and to speak with their Personal Tutors or other members of staff in their department should they have any queries about what constitutes academic misconduct. The College treats academic misconduct very seriously and misunderstanding about what constitutes academic misconduct will not be accepted as an excuse. Similarly, extenuating circumstances cannot excuse academic misconduct.

8.6.1 What is Plagiarism?

'Plagiarism' means the presentation of another person's work in any quantity without adequately identifying it and citing its source in a way which is consistent with good scholarly practice in the discipline and commensurate with the level of professional conduct expected from the student. The source which is plagiarised may take any form (including words, graphs and images, musical texts, data, source code, ideas or judgements) and may exist in any published or unpublished medium, including the internet. Plagiarism may occur in any piece of work presented by a student, including examination scripts, although standards for citation of sources may vary dependent on the method of assessment.

Identifying plagiarism is a matter of expert academic judgement, based on a comparison across the student's work and on knowledge of sources, practices and expectations for professional conduct in the discipline. Therefore it is possible to determine that an offence has occurred from an assessment of the student's work alone, without reference to further evidence.

9 Engagement Requirements

For the Information Security Group, the engagement requirements for students are:

- Submission of summative assessment for each module
- Log-in in Moodle at least once during the previous 7 days.
- Access to the additional materials posted by each of the module leaders each week.

10 Careers information

The College's Careers & Employability Service is based in the Davison Building. The careers service run a number of industry themed weeks and a range of standalone events during the academic year including a Careers Fair in October. Our events are open to all students. One to one appointments are available all through the year where you can talk over your career ideas or get your CV, cover letter or application checked. You can also book a practice, in person or video interview.

Our website and Careers Moodle has a wide range of help and information including interview skills, writing CVs and applications, assessment centres & psychometric tests.

For more information about all Careers events and appointments visit their website or come along and speak to their friendly and helpful staff.

The School of Engineering, Physical and Mathematical Sciences has a dedicated Placements and Year In Industry Administrative Officer, Supna Luthra, who is based in Bedford Building, room 1-29 and can be contacted at supna.luthra@rhul.ac.uk
10.1 Placements

For Year-In-Industry students, information about placements is circulated via Moodle and Facebook.

11 Health and Safety Information

The Health and Safety webpage provides general information about our health and safety policies.

11.1 Code of practice on harassment for students

The College is committed to upholding the dignity of the individual and recognises that harassment can be a source of great stress to an individual. Personal harassment can seriously harm working, learning and social conditions and will be regarded and treated seriously. This could include grounds for disciplinary action, and possibly the termination of registration as a student.

The College’s Code of Practice on personal harassment for students should be read in conjunction with the Student Disciplinary regulations and the Complaints procedure.

11.2 Lone working policy and procedures

The College has a ‘Lone Working Policy and Procedure’ that can be found here.

Lone working is defined as working during either normal working hours at an isolated location within the normal workplace or when working outside of normal hours. The Department and the type of work conducted by students is classified as a low risk activity and as such the following advice is relevant.

Any health and safety concerns should be brought to the attention of the Departmental Health and Safety Coordinator or the College Health and Safety Office.

It is likely that most activities will take place on College premises. However, the principles contained in the above section will apply to students undertaking duties off campus.

12 Department codes of practice

12.1 ISG MSc Student Acceptable Use Policy (AUP)

You have been granted conditional access to the Information Security Group (ISG) and Royal Holloway University of London (RHUL) computer system(s) (henceforth known as “the computer”) for the purposes of “academic use” as defined in the “Computer Centre Regulations”.

12.1.1 Acceptance and Enforcement

By signing the acceptance of use statement on the department registration form you accept the conditions of use of “the computer” as set out in the RHUL ‘Computer Centre Regulations’ (attached) and abide by the additional conditions set out in this document. If the conditions of use are broken, access to “the computer” may be withdrawn and further action taken by the Director of the ISG.
12.1.2 Access to a Computer and Password Conventions

You have been provided with an individual user account with a unique username and initial password. When you first logon to “the computer” you will be required to change the initial password to a password of your choice. You must keep your password secure, not reveal it to others and do not share or permit sharing of user accounts. You are responsible for the security of your password and associated account(s). You will be prompted to change your password every 90 days. You may not leave an interactive user session unattended and must log out to prevent unauthorised use of your user account. It is permissible to “lock” the workstation for short time periods (less than 90 minutes) if this facility is available.

User passwords must have the following characteristics:

- Contain a mixture of upper and lower case letters (e.g. A-Z, a-z)
- Contain at least one (1) digit and one (1) punctuation characters/symbols (e.g. 0-9, !@#$%^&*()_+~{}[]:;'?><,./)
- Contain at least eight (8) characters
- Not contain any word in any language, slang, dialect, jargon etc.
- Are not based on personal information, username, names of family etc.

Passwords must never be written down or stored in unencrypted electronic form. Guidance on choosing a good password that is memorable:

- Think of a phrase, for example “the quick brown fox jumps over the lazy dog”.
  - Take the first letter of each word in the phrase (“tqbfjotlz”) OR
  - Take the last letter of each word (“eknxsr eyg”) OR
  - Take the first letter of some words and the lengths of other words (“t5b3j4t4d”)
- Substitute digits and punctuation characters/symbols to produce a password that conforms to the password policy, e.g. (“t5b!j4t4d”)

12.1.3 Prohibited Use and Access to Content

You may not use “the computer” to:

- send to another any message or other electronic article which is intended to cause harassment to another, or is racist, or is indecent or grossly offensive, or contains a threat, or is information which is false or believed to be false
- commit any offence of forgery, theft, fraud, blackmail, or any other criminal offence prohibited by an Act of Statute in the United Kingdom
- send out mass mailings to promote any material other than that which directly relates to your academic studies
- infringe the copyright held on any material (including but not limited to; software, books, journals, music, films, images etc.)
- download and install executable code (excluding mobile code; e.g. Java/.NET) without prior consent from the ISG Network Manager or ISG Systems Administrator
- carry out port scanning or security testing, except where prior consent has been given in writing by the ISG Network Manager for specific network(s) and host(s)
- circumvent or otherwise disable security or audit controls, including but not limited to; antivirus, firewalls and audit software.

You may not use ‘the computer’ to access, or enable the access, to any material (whether in a removable storage medium or not) containing the following:
• Any computer material of a sexual or indecent nature
• Any images or text that denotes violence to humans or animals
• Any material that is racist, or promotes racial hatred
• Any material that promotes or contains a threat to the damage of property
• Any material concerning the possession, sale, supply or distribution of lethal weapons or explosives
• Any material concerning the possession, the making or the supply or distribution of prohibited drugs as defined under the Misuse of Drugs Act.


You may not cause the computer to perform any function whereby access is secured to any program or data to which you are not authorised whether the program or data relates to this computer or any other computer. You may not commit, or enable the commission of, any unauthorised act to impair the operation of this computer, or prevent or hinder access to any program or data held in this computer, or impair the operation of any such program or the reliability of any such data.

12.1.5 Using the Computer to Make Purchases

The RHUL e-mail account may not be used to make any purchases over the Internet. Where it is necessary to make purchases on-line over the Internet access is authorised to other email accounts where purchase transactions may take place. It is understood that the ISG / Royal Holloway take no responsibility for the security of on-line transactions or the purchase of any material or goods.

12.1.6 Prevention, Detection and Investigation of Misuse

The Regulation of Investigatory Powers (RIP) Act 2000, the Lawful Business Practice Regulations (2000), and the Information Commissioner Code on Monitoring at Work (2003) provide the ISG / Royal Holloway the right to access all material, including email, held on the ISG / Royal Holloway computing facilities (“the computer”) where abuse is suspected or where there is a pressing academic or business need. Communications on or through the ISG / Royal Holloway computer systems (“the computer”) may be monitored or recorded to secure effective system operations and for other lawful purposes.

Please note that the content of individual communications and files is not routinely monitored. However the ISG / Royal Holloway does reserve the right, within the law, to monitor in detail if there is some evidence of illegal or serious misuse of facilities, or if provision of the service may be compromised.

The person having the right to control the operation and the use of this private telecommunication system is the Director of Information Services, the Director of the ISG (or deputy), the ISG Network Manager and the ISG Systems Administrator.

Revision 1.0 – 22/09/08 - Initial Issue - Jon Hart, ISG Network Manager

Policy approved 23rd September 2008 by Professor Peter Wild (Former) Director of the ISG.