

## PROGRAMME SPECIFICATION

This document describes the **Postgraduate Diploma and Postgraduate Certificate in Information Security**. This specification is valid for new entrants from **September 2011**.

The aims of the programme are:

- to provide staff already employed in information security with an opportunity for further professional development at postgraduate level;
- in utilising students' professional experience, the taught component of the programme will develop a comprehensive knowledge and critical understanding of the different risks to the security of business information and information systems, together with strategies and methods by which these risks may be eliminated or minimised;
- by undertaking an extended research project related to their employment, students will further develop their analytical and problem solving skills in relation to a specific problem in information security (only for candidates progressing to the Postgraduate Diploma stage).

This programme is only offered for part-time study, normally lasting four years, for professional staff who are already in employment in information security and related areas of business and commerce, government and military. It consists of a number of compulsory and optional taught courses, which are delivered in-house by a team of experienced professional practitioners and Royal Holloway staff, followed by an individual project dissertation carried out under the supervision of a member of the Royal Holloway Information Security Group. Courses may also be delivered off-campus and on an accelerated schedule by arrangement.

This document provides a summary of the main features of the programme, and of the outcomes which a student might reasonably be expected to achieve if full advantage is taken of the learning opportunities provided. Further information is contained in the College prospectus, the College Regulations and in various handbooks issued to students upon arrival. Whilst Royal Holloway keeps all its information for prospective applicants and students under review, programmes and the availability of individual courses are necessarily subject to change at any time, and prospective applicants are therefore advised to seek confirmation of any factors which might affect their decision to follow a specific programme. In turn, Royal Holloway will inform applicants and students as soon as is practicable of any substantial changes which might affect their studies.

### **Learning outcomes**

In general terms, on completion of the programme students will be able to demonstrate the following learning outcomes, differentiated by the orientation (systems and technical security or security management) chosen:

#### *Knowledge and understanding*

- different types of security risk associated with information and data within IT-based businesses, models for risk and threat assessment, and the range of possible countermeasures;
- essential principles and concepts relating to effective information security management within an organisation, including issues of information ownership, access and use;
- different information security models, and the key strategies, systems, procedures, and techniques used to protect the security of business information and detect its misuse;
- principles of cryptography, and the different types of cryptographic algorithms;
- legislation, regulations, and treaties related to information security and privacy, and the implications for IT-based businesses;
- current and emerging national and international standards, frameworks and guidelines for the management of information security;
- current business and technical environments in which information security management operates along with implications for best practices

#### *Skills and other attributes*

- analysing and assessing the risks to a business in storing and transmitting information;

- applying knowledge and understanding of information security management principles, and the relevant legislation, to the development and maintenance of appropriate security policies, standards and procedures;
- selecting the most appropriate tools and methods to protect the security of information within an organisation;
- understanding the principles and requirements for cryptographic algorithms and protocols used for protecting the security of information;
- analysing a range of specific security threats and devising appropriate systems and methods to combat them;
- designing and integrating information security procedures and tools in a system and network environment;
- designing and developing a flexible and effective security structure to meet the diverse security needs of business organisations, including those involved in electronic commerce;
- devising strategies to cope with computer misuse, information security incidents and maintaining business continuity management;
- devising an effective staff training programme to promote awareness of information security risks and measures to combat these, including defining individual roles and responsibilities;
- devising systems for monitoring the effectiveness of the information security measures employed within an organisation;
- planning and carrying out a project requiring a degree of original research into a defined problem in some aspect information security under suitable guidance;
- writing a research report to an appropriate professional format and standard, to include a critical evaluation of relevant published literature, and the formulation, testing and evaluation of an original hypothesis;\*
- abstracting and synthesising information from different written and electronic sources;\*
- evaluating critically published research papers, reviews and articles;\*
- assessing the merits and limitations of alternative theories, policies and systems;\*
- evaluating critically alternative methodologies and techniques, critically diverse or contradictory evidence and making sound judgements;\*
- analysing and solving problems, displaying initiative and originality in tackling problems;\*
- interpreting critically qualitative and quantitative data, and proposing hypotheses to explain new data;\*
- ability to assess the available, and sometimes incomplete, evidence and to make reasoned judgements, arrive at sound decisions and develop a coherent argument;\*
- ability to present complex qualitative and quantitative information clearly and concisely, both orally and in written forms;\*
- a commitment to applying and achieving the appropriate professional standards in the work situation;\*
- ability to work autonomously, with initiative and to assume responsibility for planning and implementing strategies to achieve stated goals and completing tasks to a high professional standard, or alternatively to work effectively within a team;\*
- motivational skills to promote appropriate information security strategies within the student's own business organisation;
- a commitment to continuing professional development and learning.\*

(\* denote transferable skills)

[Back to top](#)

### Teaching, learning and assessment

Teaching and learning in the programme are closely informed by the active research of staff, particularly in the areas of information security management, network security, systems security, digital forensics cyber security, and cryptography. The above learning outcomes will be developed through a combination of lectures, group discussions, syndicate exercises, case studies of 'real life' problems, practical demonstrations and IT workshops. The emphasis throughout will be on the active participation of students and (where appropriate) the sharing of their experience in information security. For the research project, learning is by independent research and private study, supported by research supervision. Assessment is by completion of coursework essays and the research project, while formative assessment will also include in-course exercises and presentations. Full details of the assessments for individual courses can be obtained from the [Information Security Group](#).

[Back to top](#)

### **Details of the programme structure(s)**

The precise programme of taught courses will depend to some extent on each student's professional experience and interests but will normally consist of the following:

#### **Course titles and duration**

##### **Compulsory core course units**

Students must take:

Managing Information Security - 3 days

Risk Assessment - 2 days

Cryptography - 2 days

Plus

##### **Optional Course Units**

A selection to be made from courses within each of the following two areas (at least one course from each and a minimum of eight days – in case of accelerated groups these may be pre-arranged for an entire group; note that not all modules may be offered regularly):

#### **A: Information Security Management**

Cyber Crime - 2 days

Human Centred Security - 2 days

Incident Response and Investigations - 2 days

Information Security Law and Regulations - 1 day (generally not offered for overseas groups)

Security Standards & ISO/IEC 27001 - 2 days

#### **B: Systems and Technical Security**

Advanced Digital Forensics - 2 days

Applied Cryptography - 2 days

Foundations of Digital Forensics - 2 days

Identity Management - 2 days

Key Management and PKI - 2 days

Network Security - 2 days

Physical Security and Technical Surveillance - 1 day (generally not offered for overseas groups)

Security in Smart Card Technology - 2 days

Security Testing - 2 days

System Security - 2 days

Wireless Security - 2 days

**N.B.** Due to the dynamic nature of the subject and the rapid developments and changes in professional practice, the range and type of courses offered in any year may differ slightly from the above. Students will be notified before enrolment of any changes to the programme. A full list of optional courses for the current academic year can be obtained from the [Information Security Group](#).

#### **Project-Dissertation**

The project is a compulsory component of the programme for the award of Postgraduate Diploma. It is an independent piece of work involving critical analysis and originality in the study of a specific problem in information security. The problem chosen may be of an academic nature, such as a critical review of existing information security policies and procedures, or may be concerned with a particular practical application involving experimentation. Each student will be allocated a project supervisor from the Royal Holloway Information Security Group, and will be required to submit a dissertation, typically of a length between 50 and 100 pages. Further information is available [here](#).

[Back to top](#)

## Progressions and award requirements

In order to progress to the Postgraduate Diploma independent project, students must fulfil the attendance and assessment requirements of the course units that make up the taught part of the programme.

Assessment of the course units is by coursework essays. Depending on the combination of courses taken, students will complete three short essays (1500 to 3000 words), covering the core and each option area. The essay on the core material will be submitted first and written comments will be provided by the examiners to provide formative feedback for the remaining two essays. In order to pass the taught component of the programme, students must achieve an average of at least 50% with not less than 40% in any individual essay.

The project is assessed on the basis of the dissertation and, where appropriate, on an evaluation of any relevant materials or artefacts, such as a computer programme, which form an integral part of the project. The pass mark for the project is 50%. Students who pass both the taught component and the project will be awarded a Postgraduate Diploma in Information Security.

Students who pass the taught component but elect not to proceed to the project stage will become eligible to be awarded a Postgraduate Certificate.

Full details of programme progression and award regulations are provided in the College Regulations on the College Web Site ([Academic Regulations](#)).

[Back to top](#)

## Student support and guidance

- Programme director: The programme director meets the students during the induction meeting at the beginning of the academic year. The programme director acts as a point of contact for pastoral support and any questions about the programme throughout the year.
- Project supervisor: All students choose a supervisor with whom they meet regularly to discuss all matters relating to their project.
- Personal adviser: All students are allocated a personal adviser, with whom they meet at least once a term, and more regularly if required, to discuss all matters relating to their programme and for pastoral support.
- Representation on the Postgraduate Student Committee.
- All academic staff members are available and accessible through an open-door policy or by operating an office hours system.
- Students attend an introductory session on the Department's computing facilities, Mathematica and Minitab, and an introduction to the Library during the first week.
- Programme handbook.
- Supporting materials and learning resources in the Department, College libraries and computer centre.
- College Careers Service.
- Access to all College and University support services, including Student Counselling Service, Health Centre and the Education Support Office (for students with special needs).

[Back to top](#)

## Admission requirements

Admission to the programme normally requires a second class honours degree together with current employment in Information Security or a related field. However, applications from students with equivalent overseas qualifications or those with lesser qualifications but who possess appropriate professional or industrial experience and the motivation to succeed are strongly encouraged and will be considered on a case-by-case basis. Students whose first language is not English may also be asked for a qualification in English Language at an appropriate level. For further details please refer to the [Prospective Students](#) web page. It may also be helpful to contact the [Admissions Office](#) for specific guidance on the entrance requirements for particular programmes.

[Back to top](#)

### **Further learning and career opportunities**

The Certificate and Diploma are intended as a foundation for a professional career as well as for postgraduate research in Information Security. Graduates of the qualifications are expected to find employment in both industry and commerce as security experts, and the need for such experts is likely to be high for the foreseeable future. Our graduates are highly employable and, in recent years, have entered many different information security-related areas, including banking, telecommunications, large security consultancies, public utilities, and the retail sector. For more details on further learning and career opportunities please refer to the [Careers Service](#).

[Back to top](#)

### **Indicators of quality and standards**

The Programme is offered by the Information Security Group, which is part of the Mathematics Department. The Information Security Group at Royal Holloway is one of the leading providers of postgraduate training programmes in information security for industry, and was the first Academic Faculty to offer full-time and part-time Masters Degrees in this subject. Since its inception in 1992 the ISG has expanded its Masters programme, increased its staff, research and students to become the prime U.K. provider of academic qualifications in the U.K.

The ISG is one of the largest academic groups of security researchers in the world and all members of the group have strong links with external organisations involved with information security and secure electronic commerce, including many of the largest such organisations in the country.

Royal Holloway's position as one of the UK's leading research-intensive institutions was confirmed by the results of the most recent Research Assessment Exercise (RAE 2008) conducted by the Higher Education Funding Council (HEFCE). The new scoring system for the RAE 2008 measures research quality in four categories, with the top score of 4\* indicating quality that is world-leading and of the highest standards in terms of originality, significance and rigour. 60% of the College's research profile is rated as world-leading or internationally excellent outperforming the national average of 50%. The College is ranked 16th in the UK for research of 4\* standard and 18th for 3\* and 4\* research.

[Back to top](#)

### **List of programmes with details of awards, teaching arrangements and accreditation**

The programme is taught by staff at Royal Holloway, University of London and by a team of experienced professional practitioners and leads to an award from Royal Holloway and Bedford New College.

#### **Postgraduate Diploma programmes in Information Security**

Postgraduate Diploma in Information Security (QCC) (1223)

#### **Postgraduate Certificate programmes in Information Security**

Postgraduate Certificate in Information Security (QCC) (2150)

[Back to top](#)