# Programme Specification

A Programme Specification provides a concise summary of the main features of a programme and its intended learning outcomes. It is intended to be used by prospective students, current students, academic staff and potential employers.

| Programme Title: | |
|---|---|
| **MSc Cyber Security** | |
| **Programme (AOS) Code(s):** | **MT1CYS7** |
| **UCAS Code:** | **N/A** |
| **Name of Final Award:** | **Master of Science, MSc** |
| **Level of Qualification:** | **Level 7** |
| **Regime of Delivery:** | **Attendance** |
| **Mode(s) of Delivery:** | **Full Time** |
| **Typical Length of Study (Years):** | **1 Year** |
| **Professional Body Recognition / Accreditation (including specific requirements where applicable):** | **N/A** |

## Brief Description of the Programme

The security concept is a rapidly growing element of the industry sector due to the significant increment information, privacy and system breaching and attacks. There are many skills required of adept and effective security specialists, who may be responsible for sensitive activities, information and projects.

This programme is designed to provide prospective and practicing cyber security specialists with a range of skills and develop knowledge in order to be able to operate with confidence within the cyber security sector. It aims to meet the needs of students who want to improve their technical and managerial security skills, and to access a Master's degree-level qualification in Cyber Security. The programme will provide a combination of studies of subject areas which will provide a solid educational basis for the technical and management cyber Security solutions.

The programme is to provide students with an academically rigorous, relevant and industry-related program which will allow them to provide business-orientated security experience based upon knowledge, best practice and regulatory guidance.

As one of leading industrial countries, the UK has considered cyber security as one of the most important concepts for providing safe and reliable products and service. Therefore, the UK prioritises Cyber Security and aim to become the world leader in the cyber security sector.

The MSc Cyber Security program is designed for graduates, managers, IT and Business specialists looking to understand, develop or apply cyber security solutions in a strategic, technical, business, consultancy or management context. It has been designed to suit those from a range of backgrounds including; computing, IT, and business or management background.

The course is focused to cover both technical and management aspects needed in the cyber security sector. The balance between the two perspectives will give the students the ability to act as security specialists in both areas, and to increase and enhance their employability prospects.

**Distinguishing Features**

- This program has been structured to include highly demanded technical and management security technologies, trends and polices to prepare learners/students for work in this fast-moving sector
- This program suits for learners who look to develop themselves professionally, or who wish to return to or continue their education in a manner which will enhance their professional standing.

## Programme Aims

| | |
|---|---|
| 1 | Develop a high level of theoretical and practical knowledge in cyber security |
| 2 | Enable students to become capable in a range of cyber security skills, tools and solutions |
| 3 | Respond to the demands of the developing cyber security market |
| 4 | Develop skills in independent learning, decision making and research in cyber security |
| 5 | Improve leadership and management skills to enable the effective management of security systems and business positions in the cyber security sector. |

## Programme Learning Outcomes

The Bucks Graduate Attributes focus on the development of innovative leaders in professional and creative capacities, who are equipped to operate in the 21st Century labour market and make a positive impact as global citizens. The attributes are developed through the programme.

| ID | Learning Outcome |
|---|---|
| **Graduate Attribute: Knowledge and its application (K)** | |
| K1 | Critically evaluate global contemporary issues relating to Cyber Security techniques, management, and solutions |
| K2 | Demonstrate critical consideration of key concepts, issues and theories related to the development, management and marketing of security businesses |
| K3 | Consolidate and synthesise a coherent body of knowledge in order to execute a sustained piece of independent work using appropriate media |
| K4 | Critically apply appropriate solutions to cyber security problems. |
| **Graduate Attribute: Creativity (C)** | |
| C1 | Critically evaluate arguments, assumptions, abstract concepts and data to make creative informed judgments |
| C2 | Wisely apply theory to practice in the strategic management and technical solutions of security systems within organisations |
| C3 | Judiciously select effective solutions in the development of appropriate security systems |

| | |
|---|---|
| **Graduate Attribute: Social and ethical awareness and responsibility (S)** | |
| S1 | Critically evaluate arguments, assumptions, abstract concepts and data to provide best technical/managerial consultation, decisions and/or solutions. |
| S2 | Critically consider how ethical and cultural values - including the student's own - have an impact on responses to and rival interpretations of security and related subjects |
| S3 | Synthesise and evaluate information from a wide variety of sources relating to cyber security and business issues |
| **Graduate Attribute: Leadership and self-development (L)** | |
| L1 | Develop theoretical and practical strategic management and technical solutions of security systems within organisations |
| L2 | Critically evaluate theories, principles, concepts and factual information in the development of solutions to cyber security problems |
| L3 | Demonstrate confident leadership in building and developing efficient security systems in response to cyber security problems |

## Programme Structure

Programmes are structured in stages. The number of stages will vary depending on the mode (e.g. full-time, part-time), duration and location of study which will be detailed in the Programme Handbook.

Modules are set at a specific academic level and listed as either core (compulsory) or optional. The level indicates the relative academic difficulty which will increase through the programme. Passing modules will reward you with academic credit. The amount of credits will depend on the complexity of the module and the level of effort required, which is measured in 'notional learning hours'.

Our Academic Advice webpages provide more information on the structure of taught awards offered by the University.

*Please note: Not all option modules will necessarily be offered in any one year. Other option modules may also be introduced at a later stage enabling the programme to respond to sector developments.*

### Level Seven

| Code | Module Title | Credit | Core / Option | Compensable (Normally Yes) |
|---|---|---|---|---|
| CO701 | Risk Management and Cyber Security Assurance | 15 | C | Yes |
| CO702 | Mobile and Information Systems Security Management | 15 | C | Yes |
| CO703 | Cyber Security in Network Systems | 30 | C | Yes |
| CO704 | Cloud Security | 15 | C | Yes |
| CO705 | Business Continuity and Disaster Recovery | 15 | C | Yes |
| CO706 | AI Based Security Systems | 30 | C | Yes |
| CO707 | Project | 60 | C | No |

## Learning and Teaching Activities

Please see the Academic Advice pages for a description of learning and teaching activities that are recognised by the University. Detailed information on this specific programme is outlined below:

The MSc Cyber Security programme provides varied learning and assessment activities. Modules on this programme will be taught in line with best practice across the university and in the sector. A variety of approaches, and good use of the latest technology, will be blended together to engage students in learning in class and beyond, and to encourage full student participation. The course team will strive to ensure that all modules embrace current industrial practice wherever possible.

A range of teaching methods will be used including:

**Lectures**
This is the most formal teaching strategy employed in teaching the modules. It is generally used to deliver a body of theoretical information to a group of students and is most effective when followed up by a seminar, practical or tutorial session to consolidate learning.
The lecture format may be supported by written hand-outs, slides, web or library references which serve to reinforce and expand the audio-visual information presented. In addition, staff will make appropriate use of the VLE (Blackboard) facilities or any other appropriate facility. This should enable lecturers to enhance the traditional communication and learning mediums, as well as making material available to students at home and university.

**Tutorials / Practical Sessions**
Often in smaller groups, tutorials are guided learning sessions, which can either support a formal lecture by students working through tutorial sheets with the help of a lecturer or by students working through practical exercises in say a computing room.

**Seminars**
These can vary from large group seminars, which provide an opportunity for the student-led formal debate of particular topic areas, to 'impromptu' discussion sessions with smaller groups, which may for example follow the showing of a video.

Other techniques such as industrial visits, guest lectures and computer aided learning tools such as the university's VLE will be used where appropriate. This variety of techniques is aimed at stimulating student learning. The teaching and learning strategies for individual modules are detailed in the relevant module pro-forma.

### Additional Course Costs

There are costs associated with all studies, additional to the tuition fee, which require consideration, when planning and budgeting for expenditure. Costs are indicative and for the total length of the course shown unless otherwise stated and will increase with inflation; depending on the programme they may include equipment, printing, project materials, study trips, placement activities, DBS and/or other security checks.

industrial visits – cost to be confirmed

### Contact Hours

1 unit of credit is the equivalent of 10 notional learning hours. Full time undergraduate students study 120 credits (1200 hours) and full-time postgraduate students study 180 credits (1800 hours) per year or 'stage' of the course.

| Course Stage | Scheduled Activities (Hours) | Guided Independent Study (Hours) | Placement / Study Abroad (Hours) |
|---|---|---|---|
| **Year One** | 234 | 1566 | N/A |

## Assessment Methods

The Assessment and Examination webpages provide further information on how assignments are marked and moderated, including a description of assessment activities. These also include further information about how feedback on assessed work is provided to students, including our commitment to ensure this is provided to students within 15 working days (the 'three-week turnaround').

The majority of the assessment within the MSc Cyber Security course comes from module coursework or team projects appropriate to the module itself. Module coursework will naturally vary across modules, but is likely to be representative of the following assessment types: essay writing; report writing; artefact construction (a technical design and development project using appropriate software and/or code); portfolio construction (task based, comprising report writing and the technical design/development of code or a software based artefact). Some modules will also make use of individual and group project presentations.

**Referral Opportunities**

As with any award at Buckinghamshire New University, if a student has not received a pass mark (normally 40%) for a module or piece of assessment, they may be required to be reassessed in the component(s) that they have failed.

### Classification

| | |
|---|---|
| **Calculation of final award:** | **100% Level 7** |

For full details of assessment regulations for all taught programmes please refer to our Results webpages. These include the criteria for degree classification.

## Admissions Requirements

Please see the Application webpages for more information on how to apply, including a statement on how we support students from a variety of backgrounds. Please also see our general entry requirements for taught programmes. Applicants who do not meet our published entry requirements are encouraged to contact our admissions team for further advice and guidance.

### Typical applicant profile and any programme-specific entry requirements

Applicants will be primarily assessed on their academic qualifications although some previous experience in computing, IT, business or management is desirable as part of the candidate's overall profile. A typical offer will include a 2.2 Honours degree or equivalent qualification acceptable to the University in Computing, Web Development, and Computer Science; Software Engineering, System Engineering, and Mathematics with Computer Science; or Physics with Computer Science, or a related discipline.

Applicants are expected to have mathematical ability and computer science experience as evidenced either through the content of their primary degree or through another appropriate formal qualification. It would be beneficial if applicants have experience programming in C and working in a Linux environment.

We also consider applications from those who have gained relevant skills through a wide range of vocational qualifications or responsible experience and experiential learning for mature applicants (subject to an interview).

English Language Requirements:
TOEFL Internet test: 87 (R22, L21, S23, W21)

### Opportunities for students on successful completion of the programme

Cyber Security graduates will have an in-deep understanding and knowledge of how to analyse and protect variant system applications against different threats and risks, and have the capability to consult on and develop security systems. On successful completion of the programme, students will be well place to provide and manage solutions to security problems in systems and networks.

The MSc in Cyber Security will enable graduates to take on a range of roles that include System Security Specialists, Cyber Security Engineers, System Security Analyst/Architects, Information Analysts, or Architects. The most common job titles, according to the SANS Institute Cybersecurity Professional Trends survey, are Security Analyst, Security Engineer or Architect, Security/IT Director or Manager, CISO/CSO, Systems Administrator, Network Architect or Engineer, Forensics Investigator, Auditor, Systems Engineer or Integrator.

### Recognition of Prior Learning

Previous study, professional and / or vocational experiences may be recognised as the equivalent learning experience and permit exemption from studying certain modules. Please refer to our Credit Accumulation webpages for further guidance.

## Student Support

During the course of their studies, students will be supported in the following ways:

- At the start of their studies all students will receive a full **induction** to the programme which will include introduction to the staff responsible for delivering the course, and access to library and IT facilities
- The **Programme Handbook** will outline the exact nature of the course and how it is structured, including the availability of option modules

- Each student will be allocated a **Personal Tutor** who will support their academic development, be able to advise and guide them with their studies and, where necessary, give advice on study options
- Students will be able to access our full range of **support services**, including the Learning Development Unit for skills and study support, the Library, the Careers and Employability Team, Student Finance Team, Accommodation and Counselling Services

# Appendices

## Quality Assurance

| | |
|---|---|
| **Awarding Body:** | **Buckinghamshire New University** |
| **Language of Study:** | **English** |
| **QAA Subject Benchmark Statement(s):** | **Master's degrees in computing, 2011** |
| **Assessment Regulations:** | ***Academic Assessment Regulations*, accessible via the Academic Advice webpages (https://bucks.ac.uk/students/academicadvice)** |
| **Does the Fitness to Practise procedure apply to this programme?** | **No** |
| **Date Published / Updated:** | **01 May 2018** |

## Other awards available on programme (Exit Qualifications)

Please refer to the *Academic Qualifications Framework* for Exit Qualifications recognised by the University and credit and module requirements.

| | |
|---|---|
| **Name of Exit Qualification:** | **Postgraduate Diploma (PGDip)** |
| **Full name of Qualification and Award Title:** | **PG Dip Cyber Security** |
| **Credits requirements:** | **120 Credits** |
| **Module requirements:** | **ALL 120 Credits at Level 7**<br>• **CO701**<br>• **CO702**<br>• **CO703**<br>• **CO704**<br>• **CO705**<br>• **CO706** |

| **Learning Outcome** |
|---|
| Identify and discuss global contemporary issues relating to Cyber Security techniques, management, and solutions |
| Demonstrate critical consideration of key concepts, issues and theories related to the development, management and marketing of security businesses |
| Critically evaluate arguments, assumptions, abstract concepts and data to make informed judgments |

| | |
|---|---|
| **Name of Exit Qualification:** | **Postgraduate Certificate (PGCert)** |
| **Full name of Qualification and Award Title:** | **PG Cert Cyber Security** |
| **Credits requirements:** | **60 Credits** |
| **Module requirements:** | **60 Credits at Level 7**<br>• **CO701**<br>• **CO702**<br>• **CO703**<br>• **CO704**<br>• **CO705**<br>• **CO706** |

| **Learning Outcome** |
|---|
| Identify and discuss global contemporary issues relating to Cyber Security techniques, management, and solutions |
| Demonstrate critical consideration of key concepts, issues and theories related to the development, management and marketing of security businesses |
| Critically review, consolidate, and synthesise to execute a sustained piece of independent work using appropriate media |