PROGRAMME SPECIFICATION

1. Key Information

Programme Title:	MSc Cyber Security
Awarding Institution:	Buckinghamshire New University
Teaching Institution(s):	Buckinghamshire New University
Subject Cluster:	Computing
Award Title (including separate Pathway Award Titles where offered):	MSc Cyber Security
Pathways (if applicable)	N/A
FHEQ level of final award:	7
Other award titles available (exit qualifications):	Postgraduate Certificate Postgraduate Diploma
Accreditation details:	N/A
Length of programme:	1 year
Mode(s) of Study:	Full Time
Mode of Delivery:	In person (on-site) delivery
Language of study:	English
QAA Subject Benchmark(s):	Computing (including Master's) (2022)
Other external reference points (e.g. Apprenticeship Standard):	British Computer Society
Course Code(s):	MSCYBSFT/MSCYBSDF
UCAS Code(s):	
Approval date:	01 December 2022
Date of last update:	

2. Programme Summary

The expanding area of Cyber Security and Resilience in the computing field is being strongly promoted by the UK government's Industrial Strategy as a prime focus for the future of the country's security development. This along with the growing need for graduates with an expertise in cyber security and resilience area for many contexts, such as business, health, education. It is at the heart of technological innovation and is a critical aspect within the technologies that are rapidly transforming traditional industries. The ever growing area of cyber security offers many exciting opportunities to be at the forefront of important area of technological developments that is directly affecting society in many vital areas. This course has been designed to incorporate guidance from the Communications-Electronics Security Group (CESG), a group within the UK Government Communications Headquarters (GCHQ),

as well as the Institute of Information Security Professionals' (IISP) Information Security Skills framework. As a professional graduate with an understanding of Cyber Security you will be in the perfect position to pursue an exciting career fully exploiting the security knowledge that underpins so much of the modern technological world.

This programme is aimed at you if you wish to develop an advanced understanding of cyber security and a desire to undertake an important role in the industry through an understanding of the deeper theoretical problems in secure contemporary computing within a range of contexts. The course provides a balance of theory and practice, providing opportunities to apply knowledge into real projects where possible. You will acquire a range of skills and competences such as the ability to think critically and computationally, critical for dealing successfully with complex real-life, practical problems. You will be exposed to a variety of computing discipline areas, so that you will then be able to select and apply appropriate principles, theories, best practices and appropriate technologies to address the needs of different computer security contexts, for a range of users, customers and stakeholders.

This programme is designed to provide and develop an advanced understanding of cyber security and a desire to undertake important roles, in the industry with confidence within the sector at this level, through an understanding of the deeper theoretical problems in secure contemporary computing within a range of contexts. It aims to improve your 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 of cyber security solutions.

The programme is to provide learners 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. Following on from this you will develop your abilities to think strategically about dynamic real-world problems, whilst enhancing and extending your transferable skill set to include analysis, design, research and leadership.

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 learners 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/learners for work in this fast-moving sector

- This program is suitable 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.

3. Programme Aims and Learning Outcomes

Programme Aims

This programme aims to:

1. Provide learners with a deep advanced understanding of the methodologies, technologies and techniques used within the field of cyber security provision and the development of an awareness of various essential technologies related to its provision in relation to commercial technical decisions
2. Enable learners to apply knowledge of cyber security and related engineering principles to the development of systems and software for industrial, business, and commercial applications
3. Make our learners aware of the impact, challenges presented, and the increasing pervasiveness and ubiquity of Cyber security issues in our contemporary world. Develop learners who can systematically and critically analyse and discriminate between options
4. Develop learners to be flexible and learning independent to evaluate different approaches to solving problems and taking technical decisions using cyber security systems, within a constantly changing complex and dynamic professional environment. Enable the building of solutions using different technologies, architectures and appropriate methodological approaches in cyber security problems and devise appropriate solutions within the context of varying organisational structures
5. Develop an appreciation of professional, moral and ethical issues involved in cyber security systems development, within a legal framework, and a sensitivity to changes in the cyber security sector through enhanced leadership, management skills and nascent sector research understanding.

Programme Learning Outcomes

Knowledge and Understanding (K)

On successful completion of the programme, you will be able to:

ID	Learning Outcome
K1	Demonstrate the fundamentals and underlying theory of computer science, based systems in the world-wide context of cyber security and information security.
K2	Describe and comment upon aspects relating to the computational principles that underpin cyber security and information security based systems, including computability, algorithmic complexity where appropriate related discipline areas.
K3	Recognise the need for the efficient as well as effective management of the process of cyber security and information security based systems and software construction within an ethical framework. Appreciating the uncertainty, ambiguity and limits of knowledge (business, industrial and commercial context) in which cyber security is deployed, and its usability.
K4	Describe and comment upon aspects of current good practice, research, leadership and management through advanced scholarship prevalent in the cyber security and information security based systems life-cycle, alongside their outputs and dependencies between stages.

Analysis and Criticality (C)

On successful completion of the programme you will be able to:

ID	Learning Outcome
C1	Determine advanced level skills of an intellectual, analytical, creative and problem-solving nature in the context of cyber security and information security based systems.
C2	Deploy innovative plans, approaches and solutions to cyber security and information security issues within a quality assurance and testing framework focused against the needs of security critical based system.
C3	Evaluate concepts and data, to make judgements, and to frame appropriate questions to achieve an appropriate solution to a problem in a logical, analytical and ethical manner across the spectrum of cyber security and information security based system developments.
C4	Assess competently and critically the analyse and use of current and future technologies in the cyber security and information security field. Apply theory to practice in the strategic management and technical solutions of security systems within organisations
C5	Evaluate critically cyber security and information security systems in terms of security risks or safety aspects, quality and associated trade-offs, whilst appreciating society's increased dependence on cyber security and information security systems technology.

Application and Practice (P)

On successful completion of the programme you will be able to:

ID	Learning Outcome
P1	Produce a final year dissertation involving the key processes of analysis, design, implementation and testing; underpinned by their associated product documentation. Applying the methods and techniques that they have learned to review, consolidate, extend and apply their knowledge and understanding of the unique challenges associated with the development and deployment of cyber security and information security based systems.
P2	Devise and sustain social, ethical and computational arguments and/to solve problems, using ideas and techniques, some of which are at the forefront of cyber security and information security discipline.
P3	Apply professional codes of conduct and appreciate the ethical considerations that underpin the acceptance and adoption of cyber security and information security systems in society by professionals, individuals and society in general.
P4	Apply the methods and techniques of requirements analysis, specification and prototyping, implementation, testing, integration, documentation, delivery and maintenance and their roles in reviewing, consolidating, extending and applying their knowledge and understanding to identify practical security requirements.
P5	Synthesise and evaluate information from a wide variety of sources relating to cyber security and business issues. Critically evaluate arguments, assumptions, abstract concepts and data to provide best technical/managerial consultation, decisions and/or solutions.

Transferable skills and other attributes (T)

On successful completion of the programme you will be able to:

ID	Learning Outcome
T1	Communicate data, ideas, problems and solutions to both specialist and non-specialist audiences effectively in writing, speaking and in appropriate forms of presentation.
T2	Apply computational data using information technology to efficiently handle such data and simulations of systems for design and testing.
T3	Consolidate and expand on previous experience in order to enhance personal development or when leading/working as part of a team.
T4	Identify the learning ability needed to undertake appropriate further training of a professional or equivalent nature.

Graduate Attributes

The BNU Graduate Attributes of: Knowledge and its application; Creativity; Social and ethical awareness and responsibility; and Leadership and self-development 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.

Whilst developing as a cyber-security and information security advanced specialist on this programme, personal attributes are developed through the practical application of analytical skills, computational principles, algorithmic intricacy, computing technology systems in a variety of creative situations, including real-world scenarios, and life-critical Case Studies. (K1, P3, P4, C1, C2, C5). Analysis and evaluation approaches are embedded throughout the programme in individual and team tasks, through the appraisal of current and past cyber security and information security-based systems supported by the feedback given to your own personal work. (P1, T1, T3, C4, P5). An understanding and awareness of operational applications fostered with a strong focus given to applying and assessing an appropriate life-cycle methodology. (K3, C4, C5). This nurtures the self-efficacy to develop your own work opportunities and to adapt to a constantly evolving technological work environment (C4, K1, K2, K4, T4). Through analysing the historical, social and cultural contexts of operational cyber security and information security systems, alongside a growing social awareness is formed to ensure professional and ethical values are developed alongside the confidence to assess existing real-world, life critical systems, whilst appreciating the balance between the needs of cyber-security practice, embedded by information security fundamentals. (P1, P2, P3, C1, T3, T2, P4, P5).

4. Entry Requirements

The University's general entry requirements will apply to admission to this programme with the following additions / exceptions:

- An academic qualification equivalent to a BSc (Hons) Degree in a relevant subject area, 2:2 classification or better
- English Language level according to current IELTS requirement

Where an applicant does not meet the standard entry requirement with regards to academic qualification, their suitability for the programme will be assessed based upon their previous studies, professional and/or vocational experiences. An interview will likely be necessary in such cases.

The accreditation of prior learning (APL) process may be utilised to determine if any exemptions from studying modules are appropriate.

5. Programme Structure

Level	Modules (Code, Title and Credits)	Exit Awards
Level 7	**Core modules:** COM7001 Cyber Security Assurance and Risk Management (20) COM7005 Business Continuity and Cyber Resilience (20) COM7002 Project (60) **Option modules:** Choose modules to the total of 80 credits: COM7006 Mobile and Information Systems Security Management (20) COM7004 Cyber Security in Network Systems (20) COM7003 Cloud Security (20) COM7007 AI Based Security Systems (20)	**Postgraduate Certificate,** awarded on achievement of 60 credits **Postgraduate Diploma**, awarded on achievement of 120 credits

6. Learning, Teaching and Assessment

Learning and teaching

Our adopted teaching and learning styles in the subject of computing reflect the role and importance that the various disciplines of the sector undertake in the modern world of today. Increasing emphasis on capability, competency and performance is woven into our approach to all aspects of our teaching and learning methods. They can reflect traditional workplace environments – placements and live projects with clients - as well as newer approaches like online evaluations, role-playing scenarios and gig-economy/commissioned work. Practical coursework, both individual and in teams, features heavily in our computing programmes.

The teaching and learning approaches in our programmes are designed to provide meaningful opportunities for applied learning in authentic or simulated work contexts, such as industrial placements. Working in teams on bigger projects simulates real-world environments and exposes learners to complexity. Ideally, projects can collaborate with industrial partners or research groups, enhancing learning and self-regulation and can expose learners to legal or ethical issues.

The focus is to provide learners better control their own educational learner journeys, giving them the tools and techniques to enable them to self-regulate and to optimise their personal performance: self-reflection, performance monitoring, evaluation and feedback within learning to support a more personalised journey. The teaching and learning approaches also aim to imbue the ability to work autonomously, both individually and in teams, reflecting the key desired professional attributes employers value in the field of computing.

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 to engage learners in learning in class, labs and beyond, and to encourage full learner participation. Meanwhile, the Course Team will strive to ensure that all modules embrace

current industrial practice wherever possible. The teaching and learning strategies employed throughout the course are those judged to be the most appropriate for each module at each stage and level of the course. The strategies have been designed to ensure that there is progression from formal teaching through to learner centred independent learning as the learner progresses through the levels of the course(s).

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 large group of learners and is most effective when followed up by a seminar or tutorial session to consolidate learning.

The lecture format may be supported by written handouts, web or library references which serve to reinforce and expand the audio-visual information presented. In addition, staff will make appropriate use of the University's VLE (Virtual Learning Environment) and rich-media facilities. This will enable lecturers to enhance the traditional communication and learning mediums, as well as making material available to learners off-site and at the university.

Tutorials / Practical Sessions

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

Seminars

These can vary from large group seminars, which provide an opportunity for the learner-led formal debate of 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 will be used where appropriate. This variety of techniques is aimed at stimulating learner learning. The teaching and learning strategies for individual modules are detailed in the relevant module proforma.

Assessment

The assessment of our Computing courses includes varied methods that are accessible to all learners. Assessments are, where possible, authentic and tied to real-world contexts and constraints, allowing learners to practically demonstrate the skills they have developed.

We aim to incorporate, where appropriate, the use of capstone activities (to encourage learners to think critically, solve challenging problems, and develop professional employability skills) when concluding the session. This brings together knowledge and practical and analytical skills that learners have developed throughout the course. This may take the form of a traditional project or end-point assessment, but other formats can be appropriate.

Where a learner may identify with disabilities that require further adjustments these will be handled, and adaptations made in accordance with the reasonable adjustment policy. The procedures used for assessment cover the subject knowledge, abilities and skills developed through the degree course.

Therefore, a variety of assessment vehicles will be used as appropriate to the module, including assignments carried out in the learner's own time, in-class assignment, workshops,

presentations and formal examination. The form of assessment has been chosen to motivate learners to achieve their best and create learning activities for the learners. The assessment vehicles for individual modules are detailed in the module descriptor.

Assessments will be appropriate to the task, achievable, motivating and vocationally focussed and will form a constructive part of the learning process.

Assessments will develop general transferable skills as well as academic skills.

Assessments will provide enough opportunity for the best learners to exhibit a level of innovation and creativity associated with excellence.

During the Foundation Year, learners will be exposed to a variety of summative and formative assessments whilst developing the academic skills to be a successful learner at university; course content and Learning Outcomes strongly relate to learners developing their knowledge and understanding of the subjects being studied and assessed.

Level 4 assessments will be primarily formative and will encourage the development of appropriate academic practice and concepts. The emphasis will be on frequent small-scale assessments wherever possible with a balance between formative and summative assessment.

Level 5 assessments will be more demanding, with the emphasis still on development of knowledge, skills, and concepts but now encouraging learning at greater depth, emphasising the fundamental principles. There will be a shift towards summative assessment.

Level 6 assessments are designed to allow learners to demonstrate their knowledge and skills so that they have become effective, independent learners. The emphasis is on summative assessment.

Advice, Feedback and Collaborative Learning

Assessment is an integral part of the education process, promoting learner learning by providing a focus for consolidating, applying and demonstrating understanding of the subject matter. The listed summative assessment regime essentially measures and grades learner development and achievement in relation to the intended Learning Outcomes. It also generates feedback information for learners about the strengths and weaknesses in their work, with tutors affirming what learners have done well whilst giving constructive and encouraging advice about areas requiring reflection and further improvement.

In fact, tutor feedback on formal assessment elements is just part of the ongoing dialogue with learners about their learning and personal development. Tutors will offer learners frequent opportunities to discuss their progress, where their work can be examined and reviewed, including the evaluation of plans and drafts for assignments prior to submission. This supportive engagement helps to clarify what “good performance” is, with reference to published criteria and expected standards; it also encourages, motivates and directs learners towards achieving their full potential.

Different strategies for timely advice and effective feedback will be adopted, according to what is fit-for-purpose for learners and modules. For instance: good or bad examples of previous learner work not only give learners clues about appropriate content, structure and presentation of assignments but also highlight common mistakes and omissions; mock exam papers and formative tests; work portfolios represent a collection of structured activities completed over a period of time with regular interactions with the tutor; individual and group tutorials; practising presentations with other learners can invite peer review; model answers can supplement and extend the feedback given on assessments; group discussions can

promote reflection and collaborative learning; audio and video recordings can be used at various points to explain topics and to give guidance; other technology (such as the VLE) can facilitate information sharing, and support learning and collaboration.

Contact Hours

One unit of credit is broadly equivalent to ten notional learning hours. Postgraduate learners will complete modules equivalent to 180 credits in total during their programme. This translates as 1800 notional learning hours. The combination of scheduled teaching (contact) activities, guided independent study and any opportunities for placement or work-based learning, will be defined at Module level.

7. Programme Regulations

This programme will be subject to the following assessment regulations:

- Academic Assessment Regulations

8. Support for learners

The following systems are in place to support you to be successful with your studies:

- The appointment of a personal tutor to support you through your programme
- A programme handbook and induction at the beginning of your studies
- Library resources, include access to books, journals and databases - many of which are available in electronic format – and support from trained library staff
- Access to Blackboard, our Virtual Learning Environment (VLE), which is accessible via PC, laptop, tablet or mobile device
- Access to the MyBNU portal where you can access all University systems, information and news, record your attendance at sessions, and access your personalised timetable
- Academic Registry staff providing general guidance on University regulations, exams, and other aspects of learners and course administration
- Central learner services, including teams supporting academic skills development, career success, learner finance, accommodation, chaplaincy, disability and counselling
- Support from the Bucks Learners' Union, including the Learners' Union Advice Centre which offers free and confidential advice on University processes.

9. Programme monitoring and review

BNU has a number of ways for monitoring and reviewing the quality of learning and teaching on your programme. You will be able to comment on the content of their programme via the following feedback mechanisms:

- Formal feedback questionnaires and anonymous module 'check-ins'
- Participation in external surveys
- Programme Committees, via appointed learner representatives
- Informal feedback to your programme leader

Quality and standards on each programme are assured via the following mechanisms:

- An initial event to approve the programme for delivery

- An annual report submitted by the External Examiner following a process of external moderation of work submitted for assessment
- The Annual Monitoring process, which is overseen by the University's Education Committee
- Review by the relevant PSRB(s)
- Periodic Subject Review events held every five years
- Other sector compliance and review mechanisms

10. Internal and external reference points

Design and development of this programme has been informed by the following internal and external reference points:

- The Framework for Higher Education Qualifications (FHEQ)
- The QAA Subject Benchmark Statement – see detailed mapping below
- The BNU Qualifications and Credit Framework
- The BNU Grading Descriptors
- The University Strategy

Mapping of Subject Benchmark Statement and any relevant Apprenticeship Standard to Programme Learning Outcomes

Subject Benchmark Statement / Apprenticeship Standard:	**Knowledge and understanding (K)**				**Analysis and Criticality (C)**					**Application and Practice (P)**					**Transferable skills and other attributes (T)**			
Benchmark / Standard requirement	**K1**	**K2**	**K3**	**K4**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**
Subject knowledge understanding and skills/ Demonstrate an exceptional understanding of the main body of knowledge for their subject and be able to exercise insightful and critical judgement in the use of that knowledge. Be creative and innovative in the application of the principles covered in the curriculum, and be able to go beyond what has been taught in classes	X	X			X	X		X	X	X		X					X	
Intellectual skills/ Critically analyse and apply a wide range of concepts, principles and practices of the subject in the context of open scenarios, showing refined judgement and	X	X	X	X	X	X	X	X	X	X	X	X	X		X			

adaptability in the selection and use of tools and techniques																	
Computational problem-solving/ Be able to demonstrate sophisticated judgement, critical thinking, research design, and well-developed problem-solving skills with a high degree of autonomy, and to create highly effective computational artefacts across complex and unpredictable circumstances		X		X	X	X	X	X		X		X		X		X	
Practical skills across the computing lifecycle/ Demonstrate the ability to undertake problem identification and analysis to appropriately design, develop, test, integrate or deploy a highly complex computing system and any associated artefacts; deeply understand the relationship between stages and be able to demonstrate related sophisticated problem-solving and evidence-informed evaluative skills	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	

Interpersonal and team working **Skills/** Demonstrate the ability to work in a highly proactive and accomplished manner, including as a leading member of a team, making excellent use of tools and techniques to proficiently communicate, manage tasks and plan projects with minimum guidance	X	X		X			X	X			X	X	X				X	
Professional practice covering Equality, diversity and inclusion, Sustainability and Entrepreneurship and enterprise education/ Identify best-of-kind practices and effect highly principled solutions within a professional, legal and ethical framework to consistently address a wide breadth of relevant considerations – including data management and use, security, equality, diversity and inclusion (EDI) and sustainability – in the work that they undertake	X				X	X	X	X	X	X		X			X	X	X	X

Mapping of Programme Learning Outcomes to Modules

Programme Learning Outcome	Knowledge and understanding (K)				Analysis and Criticality (C)					Application and Practice (P)					Transferable skills and other attributes (T)			
Module Code (Core)	**K1**	**K2**	**K3**	**K4**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**
Level 7																		
Project	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Cyber Security Assurance and Risk Management			X	X			X	X	X					X			X	X
Business Continuity and Cyber Resilience	X	X	X	X				X	X					X	X	X	X	