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:	
FDSc. Cyber Security	
Programme (AOS) Code(s):	**FU1CYS7**
UCAS Code:	**29N2**
Name of Final Award:	**Foundation Degree Science, FDSc**
Level of Qualification:	**Level 5**
Regime of Delivery:	**Attendance**
Mode(s) of Delivery:	**Full Time**
Typical Length of Study (Years):	**2**
Professional Body Recognition / Accreditation (including specific requirements where applicable):	**Not applicable to this programme.**

Brief Description of the Programme

Cyber-attacks are a serious security issue facing organisations in the information age. Today, all organisations operate with a potential information security risk and will need to implement strategies to protect their information technology (IT) systems and data. Although society has become increasingly reliant upon IT and cloud based services, cyber security skills and capability are not currently increasing at a comparable rate.

The UK takes a prominent role in cyber security provision, with the demand for new talent only set to grow in the future. This growth requires a sustained supply of competent cyber security professionals who have achieved the requisite standards and certification.

The FDSc. Cyber Security programme will provide students with a fundamental understanding of how to protect organisations, networks, IT systems and individuals against cyber-attacks and cyber threats. It will prepare them for the possibility of taking professional qualifications in their early career pathway, such as Cisco CCNA; Cisco CCNA Security; and CompTIA Security+.

The FDSc. Cyber Security programme has been developed to provide a specific opportunity for students to enter an educational programme in an increasingly vital subject area. The programme is for those wishing to develop a career as a cyber security professional, or to develop new skill sets that may enable them to consider alternative employment roles within IT services.

Prospective students will be seeking to improve their technical understanding of cyber security, IT services and risk management, and how this relates to the wider business and customer-facing needs for their future employers.

During the programme students will learn the underpinning areas of software and networked systems as well as developing specialist skills in cyber security, risk and information management.

Students will also learn to use a wide range of cyber security related tools and techniques, alongside technical skills in computer programming, software engineering, cloud and database development.

Qualified cyber security professionals are currently in high demand by business, government and law enforcement agencies across the globe. Graduating students from the programme will have gained the fundamental skills and knowledge necessary to quickly adopt the emerging technologies and concepts in this fast changing field, alongside the professional and business skills, techniques and ways of thinking needed to be able to align technical security requirements with business needs.

Programme Aims

1	Make students conversant with technical decisions relating to the commercial operation of cyber security and various types of cyber security related technologies.
2	Raise student awareness of some of the cyber security challenges and opportunities presented by the Information Age and the ubiquity of computing in our daily lives.
3	Develop students who can analyse problems, devise solutions and select the most appropriate response.
4	Develop an appreciation on the part of the student of the professional, moral and ethical issues involved in cyber security, as well as a degree of adaptability in the rapidly-changing environment.
5	Produce people who can take responsibility for planning, directing, recording and achieving their own personal and professional development.

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
On successful completion of the programme a graduate will be able to:	
Graduate Attribute: Knowledge and its application (K)	
K1	Appreciate the uncertainty, ambiguity and limits of knowledge within the core disciplines of cyber security including: information security, software security, programming, database security and network security.
K2	Apply the methods and techniques that they have learned to review, consolidate, extend and apply their knowledge and understanding to identify the practical security requirements for both computer and cloud-based systems including the recognition and analysis of criteria and models leading to specifications used in the solution of specific cyber security problems.
K3	Describe and comment upon particular aspects of the mathematical principles that underpin computer-based systems.
K4	Describe and comment upon particular aspects of current research, or equivalent advanced scholarship, prevalent in the software lifecycle, alongside their outputs and dependencies between stages, alongside the ethical, professional and legal standards required.

K5	Appreciate the uncertainty, ambiguity and limits of knowledge of the business, industrial and commercial context in which cyber security is deployed, with particular regard to its usability.
Graduate Attribute: Creativity (C)	
C1	Critically evaluate and deploy approaches to modelling in order to design computer-based information systems, with particular regard to the cyber security paradigm.
C2	Critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete), to make judgements, and to frame appropriate questions to achieve a solution, or identify a range of solutions, to a problem in a logical and analytical manner.
C3	Apply the methods and techniques that they have learned to review, consolidate, extend and apply their knowledge and understanding of the role of critical evaluation and testing in ensuring that computer-based systems are secure and meet the criteria for their defined use and future developments.
C4	Critically evaluate technical, business and human features of cyber security.
C5	Critically evaluate new and emerging computer related technologies with particular regard to cloud computing and security systems.
C6	Apply 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 secure mobile and cloud based systems.
C7	Appreciate the unique challenges associated with the development and deployment of mobile and Web-based systems.
Graduate Attribute: Social and ethical awareness and responsibility (S)	
S1	Communicate information, ideas, problems and solutions to both specialist and non-specialist audiences.
S2	Describe and comment upon particular aspects of the cyber security risks or safety aspects associated with various computer-based systems.
S3	Devise, design, develop and maintain reliable secure software and network systems, with particular regard to information systems encapsulated in a quality assurance framework.
S4	Devise and sustain arguments, and/or to solve problems, using ideas and techniques, some of which are at the forefront of the cyber security discipline.
Graduate Attribute: Leadership and self-development (L)	
L1	Deploy analytical techniques and design tools in the development of secure software and network system artefacts.
L2	Identify the learning ability needed to undertake appropriate further training of a professional or equivalent nature.
L3	Demonstrate numeracy and literacy in both understanding and presenting cases involving a quantitative and qualitative dimension.
L4	Critically evaluate a system in terms of quality and associated trade-offs.
L5	Apply the programming methods and techniques that they have learned to review, consolidate, extend and apply their knowledge and understanding to the construction and maintenance of secure software deployed on multiple platforms, using appropriate programming paradigms and languages.

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 Four

Code	Module Title	Credit	Core / Option	Compensable (Normally Yes)
CO450	Computer Architectures	15	C	Yes
CO452	Programming Concepts	15	C	Yes
CO454	Digital Technologies & Professional Practice	15	C	Yes
CO456	Web Development	15	C	Yes
CO451	Networking	15	C	Yes
CO453	Application Programming	15	C	Yes
CO403	Secure Systems	15	C	Yes
CO404	Cyber Threat and Risk Management	15	C	Yes

Level Five

Code	Module Title	Credit	Core / Option	Compensable (Normally Yes)
CO556	Network Systems	15	C	Yes
CO558	Database Design	15	C	Yes
CO506	Information Security	15	C	Yes
CO507	Cyber Security Management	15	C	Yes
CO551	Open Source Systems	15	C	Yes
CO557	Software Engineering	15	C	Yes
CO559	Intro to Intelligent Systems (Team Project)	15	C	Yes
CO508	Mobile Systems Security	15	C	Yes

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:

How will Students Learn

A variety of approaches, and good use of the latest technology, will be blended together to engage students in learning in the classroom and outside, and to encourage full student participation. The programme team will strive to ensure that all modules embrace current industrial practice wherever possible.

The teaching and learning strategies employed throughout the programme are those judged to be the most appropriate for each module at each stage and level of the programme. The strategies have been designed to ensure that there is progression from formal teaching through to student centred independent learning as the student progresses through the levels of the programme(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 students and is most effective when followed up by a seminar or tutorial session to consolidate learning.

The lecture format may be supported by written hand-outs, 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. 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 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.

How will students be assessed

A variety of assessment vehicles will be used as appropriate to the module, including assignments carried out in the student's own time, in-class assignment, workshops and presentations. The form of assessment has been chosen so as to motivate students to achieve their best, and create learning activities for the students. 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 sufficient opportunity for the best students to exhibit a level of innovation and creativity associated with excellence.

Students will be exposed to a variety of summative and formative assessments whilst developing the academic skills to be a successful student at university; programme content and learning outcomes strongly relate to students developing their knowledge and understanding of the subjects being studied and assessed.

Level 4 assessments are summative, however a large amount of formative feedback is provided in order to encourage and support the development of appropriate academic practice and concepts. The emphasis will be on frequent small-scale assessments wherever possible with a balance between formative feedback 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.

Advice, Feedback and Collaborative Learning
Assessment is an integral part of the education process, promoting student 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 students about the strengths and weaknesses in their work, with tutors affirming what students have done well whilst giving constructive and encouraging advice about areas requiring reflection and further improvement.

Tutor feedback on formal assessment elements is just part of the ongoing dialogue with students about their learning and personal development. Tutors will offer students 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 students towards achieving their full potential.

Different strategies for timely advice and effective feedback will be adopted, according to what is fit-for-purpose for students and modules. For instance: good or bad examples of previous student work not only give students clues about appropriate content, structure and presentation of assignments but also highlight common mistakes and omissions; 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 students 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.

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.

The university will provide access to the appropriate facilities and equipment to allow you to do your course. However, a student on this course may find it useful to have their own computer or laptop, so that they can work flexibly at home and elsewhere, if necessary. Whilst it is difficult to be exact, other common annual costs can be:

- Text books - £100 to £150 per year
- Software - £200 to £250 per year
- Printing - £30 to £50 per year

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 / Work Based Learning (Hours)
Year One	360	840	0
Year Two	360	840	0

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 following assessment activities are used on this programme:

- Time-constrained assessment (TCA)
- Essay or written assignment
- Report
- Project output (other than Dissertation)
- Presentation or other form of oral assessment
- Practical skills assessment
- Set exercises

Classification

Calculation of final award:	**Level 5 - 100%**

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

The FDSc. Cyber Security programme is aimed at those students wishing to acquire knowledge and competence in cyber security and secure systems development, together with the underpinning theory of computer science.

The programme provides a balance of theory and practice in information technology, systems and software engineering, alongside providing a solid foundation for further development within the graduate workplace.

Expected knowledge and skills that the entrant will have on entry to the programme: Foundation Degrees are intended to make a valuable contribution to lifelong learning by providing access to Higher Education for learners from different starting points and with different previous qualifications.

A typical offer will include GCSE Maths and English at grade C/4 or above and a UCAS Tariff score of 40-56. A minimum of two full A-levels (or equivalent) is required. Every application is considered on an individual basis.

For current information regarding our English language entry requirements, please refer to our website at: https://bucks.ac.uk/applying-to-bucks/general-entry-requirements

Do applicants required a Disclosure and Barring Service (DBS) Check?	**No**

Opportunities for students on successful completion of the programme

The programme will provide students with the appropriate skills and knowledge to pursue a number of careers within the Cyber Security and IT sectors. Including: systems security specialist; cyber security engineer; system security analyst; information analyst; security analyst; security engineer; security IT manager; systems administrator; and IT support. The programme will place great emphasis on developing the student's employability skills, thus providing them with the competence and confidence to succeed in this demanding industry.

Cyber security specialists focus on understanding risks to the security of information or data. They analyse where security breaches may occur or have occurred, and repair or strengthen systems against such breaches. This relates to the systems and networks used by companies and organisations to manage their information and information technology.

On successful completion of this award, students from all backgrounds will find their employment prospects enhanced and their understanding of the multiple facets of cyber security significantly deepened. There are multiple roles and careers available for those who have demonstrable capability in information and cyber security; and the award will allow successful students to enter the sector with confidence and evidence of subject specific knowledge and understanding. It

follows that successful students from this award will be more likely to be able to obtain employment in the component industries; and current employees will be better equipped to seek promotion and advancement. All students will have developed transferable skills that can be used in a wide range of employment roles.

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

Programme specific support (if applicable)

Not applicable to this programme.

Appendices

Quality Assurance

Awarding Body:	**Buckinghamshire New University**
Language of Study:	**English**
QAA Subject Benchmark Statement(s):	**Guidance from the QAA subject benchmark statement for Computing (there is no specific benchmark for cyber security)**
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**
Ethics Sub-committee	**Computing**
Date Published / Updated:	**September 2019**
Date programme re-approval required:	**September 2025**

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:	**Certificate of Higher Education (CertHE)**
Full name of Qualification and Award Title:	**CertHE Cyber Security**
Credits requirements:	**120 Credits**
Module requirements:	**ALL 120 Credits at Level 4**
Learning Outcome	
Comprehend and apply a simple requirement in a structured manner and implement a software solution; with appropriate application of programming techniques and coding skills.	
Demonstrate competence in the design and development of a cross-platform Web 'front-end' solution, paying appropriate attention to user expectations and process needs.	
Understand the operation of the major hardware units of computers and appreciate the fundamental components and protocols of network systems.	
Adopt a systematic approach to cyber security, as part of different environments e.g. mobile, network etc.	
Demonstrate an understanding of cyber security within a professional context, and how different tools and environments can be used for handling information security, secure communication and other purposes.	