Programme Specification

NET-CS-2016: Network Engineering (Cyber Security)

LU Foundation Degree in Science awarded by Lancaster University (FHEQ Level 5)

LU Bachelor of Science (Honours) awarded by Lancaster University (FHEQ Level 6)

Programme Status: Approved | Version: 1

Introduction

This programme specification provides a summary of the main features of the Network Engineering (Cyber Security) programme and the learning outcomes that you as a student might reasonably be expected to achieve and demonstrate on successful completion of the programme.

Further detailed information related to this programme and the College can be found in the following resources:

- Programme Handbook
- B&FC Student Handbook
- B&FC Admissions Policy
- Work based and placement learning handbook (for foundation degrees)
- Student guide to assessment and feedback

Key Programme Information

Programme Code	NET-CS-2016
Programme Title	Network Engineering (Cyber Security)
Teaching Institution	Blackpool and The Fylde College
Professional, Statutory and Regulatory Body (PSRB) Accreditation	None
UCAS Code	
Language of Study	English
Version	1
Approval Status	Approved
Approval Date	12 July 2018
JACS Code	
Programme Leader	Keith Whitehead

Programme Awards			
Award	**Award Type**	**Level**	**Awarding Body**
LU Foundation Degree in Science	Foundation Degree (240 credits)	Level 5	Lancaster University
LU Bachelor of Science (Honours)	Honours Degree (360 credits)	Level 6	Lancaster University

Programme Overview

Blackpool and the Fylde College remains committed to providing a highly responsive curriculum that is employment and future-focused and will enable you to develop the essential knowledge and skills that will prepare you for future success in work and life.

Businesses are increasingly reliant upon interconnected systems and networked infrastructures; as these systems continue to grow in size and importance, the number of job roles in computer networking increases alongside them. The need for organisations to protect themselves from the legal, political and economic ramifications derived from data losses or breaches of security is symbiotic with this reliance.

This Foundation Degree programme has produced significant numbers of graduates, the majority of whom have found employment in the area of networking. The combination of network

security with network systems administration produces extremely well qualified graduate cohorts with broad, commercially desirable skill sets and qualifications. It produces self-directing IT professionals with a wide range of career pathways available to them. Along with the technical skills referred to, you will develop your understanding of continuing professional development and the value of transferable skills.

The college has experience of delivering specialist HE networking courses linked to both the Cisco Curriculum, via the Cisco Networking Academy and the Microsoft Curriculum, via the Microsoft Academy. We have demonstrated that there is an established market for such globally recognised networking qualifications in the local area.

Building on this success, the FdSc. Network Engineering (Cyber Security) provides a specialist route in one of the most in-demand disciplines within contemporary computing.

The FdSc Network Engineering (Cyber Security) programme intends to develop technical and professional skills in order that you meet the current expectations of industry.

The skills you will develop include the ability to:

- Apply networking and hardware skills that will enable the connection, control and maintenance of various devices, using both traditional and wireless connectivity
- Protect individual systems and corporate infrastructures from unauthorised and illegal hacking and industrial espionage
- Configure, maintain and recover server based solutions to SMEs and larger corporations
- Develop specialist Cyber Security skills to prepare Information Security Professionals for a range of in-demand industry roles
- Work independently and as part of a team, the ability to take instruction and work to deadlines, communication and adaptability
- Be creative, use initiative and develop problem solving skills
- Undertake a work placement and apply the full range of technical and professional skills acquired during the foundation degree in a real world context.

The BSc. (Hons) Network Engineering (Cyber Security) programme intends to develop your advanced technical and professional competence to meet the current expectations of industry, and facilitate their adaptability to emergent requirements.

The skills you will develop include the ability to:

- Collaborate in the design and delivery of Secure Systems commissioning to provide professional guidance for both existing organisations and new entrants to the market
- Devise entrepreneurial methods for developing opportunities for SMEs and larger public / private organisations through the provision of networking and networking infrastructure
- Apply networking and hardware skills that will enable the protection of information architecture through a range of suitable security mechanisms
- Create and modify robust corporate infrastructures to protect from unauthorised and illegal hacking and industrial espionage against current and future threats
- Develop advanced creative and problem solving skills
- Work independently, in a team leading role, including the ability to issue instruction and manage workloads / task delegation with professionalism

Admission Criteria

Admission to level 4 would normally be on the basis of the applicant possessing:

For Entry prior to 2017:

A minimum of 160 UCAS Points in an appropriate discipline.

We also welcome applications from those with relevant experience in lieu of the minimum entry requirements.

For Entry from 2017 (Updated UCAS Tariff):

A minimum of 64 UCAS Points in an appropriate discipline.

We also welcome applications from those with relevant experience in lieu of the minimum entry requirements.

Only students who have studied the FdSc. Network Engineering (Cyber Security) at Blackpool and The Fylde College and achieve a PASS will be considered for this this BSc. (Honours) Top up.

Career Options and Progression Opportunities

The modules on the FdSc. will give you excellent technical expertise with understanding of organisational contexts. This will be useful for those already working in IT Support to progress to a role of Penetration Tester or Information Assurance Analyst.

When you graduate you will have the technical skills and underpinning knowledge to become:

- Cyber Security Consultant
- Penetration Tester
- IT Security Manager
- Network Security Engineer
- And many other opportunities

Upon completion of your Foundation Degree you can enhance your skills further with the specialist BSc. (Honours) Network Engineering (Cyber Security) Top up programme which is an additional year of study. Also, you may wish to pursue further Cisco qualifications or broaden your skills by studying another module here in Computing.

In addition, there is a focus on developing your transferrable skills to make you an attractive professional candidate capable across sectors.

The area of cyber security opens up many emerging opportunities in what is an area of economic growth internationally. Many evolving technology concepts including virtualisation, cloud computing, Internet of Things and mobile computing open up exciting and numerous career progression routes for you in the future.

Some of the roles that this programme will prepare you for include:

- Cyber Security Consultant
- Lead Penetration Tester
- Information Assurance Professional
- Cyber Security Contractor
- And many other opportunities

You may decide that you wish to pursue further study opportunities and performing will in this degree will provide a platform for postgraduate study (Masters / PhD) at many universities including our partner institution Lancaster University. Also, you may wish to pursue further Cisco qualifications, pursue GCHQ training or broaden your skills by studying another module here in Computing.

In addition, there is a focus on developing your transferrable skills to make you an attractive professional candidate capable across sectors.

Programme Aims

Foundation Degree programme aims:

- To provide students with a range of cyber security cognitive abilities and skills.

- To develop skills in network engineering; with regard to design, implementation, maintenance and securing network systems; thus enabling students to formulate decisions and administrate network systems.

- To develop a range of transferable skills, techniques and personal qualities that are essential for successful performance in Higher Education and in working life.

- To provide a platform for further undergraduate study.

Bachelor Degree programme aims:

- To further develop knowledge and skills to enable students to formulate managerial and strategic decisions in the administration and deployment of secure systems.

- To provide the opportunity to accurately deploy established techniques of critical analysis and enquiry in network engineering systems and security administration.

- To develop conceptual understanding which enables students to devise, develop and sustain arguments, using ideas and techniques from research and the wider subject discipline.

- To enable students to manage their own learning and to make use of scholarly reviews and primary sources.

Programme Learning Outcomes

Level 5

Upon successful completion of this level, students will be able to:

1. Identify, explain and discuss the technical and theoretical disciplines and applications involved in the development and deployment of secure systems
2. Analyse the social, legal and ethical aspects of design, implementation and evaluation of a secure system
3. Apply mathematical principles required to design, implement and maintain security mechanisms
4. Design, implement, and secure information infrastructure drawing on supporting evidence and critically analyse, select and apply suitable tools and techniques
5. Communicate information in a variety of formats to a range of audiences using a range of media which evidences both academic and digital literacy skills
6. Work effectively as an individual and as a member of a team undertaking critical self-appraisal to support continued professional development, employability, lifelong learning and transferrable skills
7. Integrate and apply essential concepts, principles and practice in the development and implementation of sustainable secure systems

Level 6

Upon successful completion of this level, students will be able to:

8. Generate ideas, concepts, proposals, solutions or arguments independently and/or collaboratively exercising critical judgement to inform system security administration practices, techniques, applications and transferrable skills
9. Employ both convergent and divergent thinking in the processes of observation, investigation, speculative enquiry and visualisation to formulate effective solutions to problems including selection of tools and techniques
10. Critically analyse and evaluate the professional, economic, social, environmental, moral and ethical issues involved in the sustainable exploitation of secure systems and apply appropriate professional, ethical and legal practices
11. Undertake critical self-appraisal and manage own learning and development identifying the need for continuing professional development and lifelong learning
12. Produce work involving critical problem identification, analysis, design and development of secure systems based on evidence which explains the relationship between these features, the need for quality and applies problem-solving and evaluation skills

Programme Structure

Pathway	Module	Level	Credits	Coursework	Practical	Written Exam
Stage 1 Stage exit award: LU Certificate of Higher Education (Awarded by Lancaster University)						
All	B4SCNET-CS: Introduction to Academic Study (Mandatory)	4	20	60%	40%	
	NET401: Network Principles (Mandatory)	4	20	50%	30%	20%
	NET402: Network Programming and Scripting Concepts (Mandatory)	4	20	100%		
	NET403: Introduction to Routing and Switching (Mandatory)	4	20	50%	30%	20%
	NET404: Introduction to Systems Security (Mandatory)	4	20	100%		
	NET405: Network Disaster Recovery (Mandatory)	4	20	75%		25%
Stage 2 Stage exit award: B&FC Foundation Degree in Science (Awarded by Blackpool And The Fylde College)						
All	BFC501-I: Work Based and Placement Learning (Mandatory)	5	20	100%		
	NET501: Project Management (Mandatory)	5	20	70%		30%
	NET502: Virtualisation and Cloud Computing (Mandatory)	5	20	50%	50%	
	NET511: Cyber Security Process Management (Mandatory)	5	20	70%		30%
	NET512: Database and Web Security (Mandatory)	5	20	100%		
	NET513: Data and Evidence Recovery (Mandatory)	5	20	100%		
Stage 3 Stage exit award: LU Bachelor of Science (Honours) (Awarded by Lancaster University)						
All	CMP601: Dissertation (Mandatory)	6	40	100%		
	NET601: Cyber Ethics and Law (Mandatory)	6	20	60%		40%
	NET602: Distributed Systems (Mandatory)	6	20	100%		
	NET603: Corporate Network Strategies (Mandatory)	6	20	70%		30%
	NET611: Cryptography and Cyber Security Trends (Mandatory)	6	20	60%		40%

Programme Delivery: Learning and Teaching

Our strategy for teaching, learning and assessment is based on good practice identified in research literature for the subject discipline. In particular we adopt an approach that will draw on your experience and that of other students to inform different approaches to practical tasks and theoretical case studies, updates content based on contemporary developments in the subject area and develops your professional skills through reflective practice.

There is an emphasis on formative assessment whereby you will have opportunities to test your skills in practical sessions and submit draft written tasks to receive written and/or verbal feedback to help you improve your work prior to final submission of assessments. The formative assessments will be delivered in the context of the module content and additional support to help you improve will be identified through our tutorial framework where your Personal Tutor will liaise with key agents throughout the college (such as Higher Education Learning Mentors) to support your development.

YEAR 1 (LEVEL 4)

At Level 4 the 'Academic and Digital Literacies' module will prepare you in research, collation and presentation of information in a range of styles to a range of audiences. This is linked to the wider subject material of the curriculum including reflection upon activities and feedback received in other modules in Semester 1. A focus on reflecting upon your work in other modules will help you improve your practice and the development of academic skills with help you achieve in future module assessments and start you well on your development of transferrable graduate skills.

The 'Network Principles' and 'Introduction to Routing and Switching' modules feature hands-on practical activities utilising NetLab equipment reinforcing concepts provided as blended (online / multimedia) learning resources by Cisco and reinforced through lecture-led discussions. Consideration is given to the environments in which these skills would be practiced in industry, inclusive of equipment selection and deployment which would be driven by business needs The 'Introduction to the Routing and Switching' module also employs the usage of Packet Tracer, which can simulate complex network architectures. This is employed as a practice tool before the application of hands-on practical skills so that particular issues can be avoided and this is also utilised to simulate more complex network architectures.

'Network Programming and Scripting Concepts' follows a similar style integrating practical activities into sessions based on demonstrations and discussions of how concepts are applied, supported by blended (online / multimedia) learning resources. Supported practical sessions on programming tasks will enable you to be supported when bugs are encountered and practice problem solving techniques to overcome coding issues. This module provides a basis for skills further developed in 'Systems Configuration and Management'

'Introduction to Systems Security' features practical activities embedded within larger scenarios with discussions on case studies considering the wider impact of security breaches including legal and ethical dimensions.

'Network Disaster Recovery' utilises case studies to help relate your understanding of concepts to real-world situations and allow for practice planning in a range of contexts. As the module moves towards the database management aspects more practical activities are integrated starting with demonstrations and then supported workshops where you will practice your skills with the ability to reflect and refine them through experience and feedback.

Overall, a largely practical approach is taken at Level 4 with an emphasis on you learning through doing, reflecting upon these tasks to develop your skills. This provides a foundation to become more critical and analytical as well as developing more complex practical skills at Level 5.

YEAR 2 (LEVEL 5)

At Level 5, the 'Project Management' and 'Work Based / Placement Learning' module are

delivered throughout the year. Themes of leadership, collaboration and organisational contexts support each other in both modules. In 'Project Management', lecture-led discussions on group dynamics and collaboration can be applied in the workplace and reflected upon. Professionalism and approaches to handling change and risks amongst other themes can be examined from these lenses. These elements of the curriculum delivery support each other in viewing concepts in different contexts allowing for deeper construction of understanding.

'Project Management' makes use of lecturer-led discussions, analysis of case studies and seminars where approaches can be shared and you can gain a better understanding of core project management issues.

'Cyber Security Process Management' makes use of lecturer-led discussions, analysis of case studies and group tutorials enabling you to share approaches with other students to the theoretical content and how it applies in real-world scenarios. 'Data and Evidence Recovery' and 'Web and Database Security' both contain a large practical element underpinned by theoretical concepts and frameworks. Lectures and lecturer-led discussions as well as reflection on blended resources are used to introduce, reinforce and reflect upon the concepts. Then more practical elements will be introduced through lecturer-led walkthroughs and supported workshops so you can hone their skills and receive feedback from the tutor.

YEAR 3 (LEVEL6)

Delivery at level six will place more emphasis on you as an independent learner and bring your research to disseminate, analyse and discuss where appropriate. There is a larger emphasis on theoretical content at Honours level and our aim will be to support you in developing high level skills such as deeper analysis, critical evaluation and reflection.

Where there are practical activities, the basics will be delivered through demonstration and supervised labs however extending the skills to achieve highly will be your responsibility; the more additional work and research you put in the better the outcomes will be for you.

This is all the more important as the dissertation will be self-managed. Supervisors will be allocated based on level of knowledge academically or technologically to aid in completion of the dissertation yet appointments need to be managed by students to build their ownership of academic progress.

The 'Cyber Ethics and Law' module explores social, legal and ethical principles. There will be some lecture-based delivery, in which you will learn about existing ethical philosophies, legislation and codes of conduct; however, the very nature of the module content requires you to take control and apply an independent approach to these topics through utilisation of current news articles and contemporary case studies to illustrate the concepts. You are encouraged to be independent and research-led bringing your contributions to the class for informed debate and discussion. Seminars will be held throughout with students leading the topics of discussion allowing various perspectives to be explored and a deeper understanding to be socially constructed.

'Distributed Systems' and 'Cryptography and Cyber Security Trends' both incorporate practical aspects as an experiential reference point to help you explore the wider context of the subject matter; this will be based on tutor-led demonstrations and practical activities which are then reflected upon in relation to fundamental theories and emerging technologies. The delivery will then move on to a more research-led format with lecture-led discussions drawing on individual professional experiences of the students. This aids in informing critical approaches to selecting, deploying and maintaining appropriate technologies for distributed systems in a range of contexts.

'Corporate Network Strategies' incorporates peer collaboration in research-led activities where groups will then make presentations or contribute to seminar sessions. Through this sharing of different approaches, effective strategic thinking and approaches can be fostered, inclusive of

critical evaluation, analysis and synthesis techniques.

The ‘Dissertation’ emphasises your self-management, information discovery and experimental practical experience. Timetabled sessions will revisit Academic and Digital Literacy skills at a higher level, emphasising scholarly activity, critical evaluation, comparison and contrast of a wide range of reliable and valid sources, data analysis techniques, structure and planning. Outside of these sessions you will need to arrange appointments with your assigned Supervisor to get one-to-one feedback and direction. The dissertation module is delivered all year and the teaching and learning approaches emphasised in the other modules aid in the development of independence and high level academic skills.

Overall, at Level 6 a more discursive approach is taken in delivery where you are expected to bring more of your own knowledge in a journey of shared discovery through subject areas. Whilst there are still lectures and activities, a much more student-led approach is utilised to build your expected graduate skills.

Programme Delivery: Assessment

YEAR 1 (LEVEL 4)

Formative Assessment

Formative assessment in ‘Network Principles’ and ‘Introduction to Routing and Switching’ utilises Cisco End of Chapter quizzes which are aligned to the Cisco curriculum and allow for an on-demand analysis of your achievement. In addition to this, formative tasks based around case study activities including network infrastructure designs, addressing schemes and example rationales are set to enable opportunities for constructive feedback ultimately enhancing your overall achievement. Within sessions there are practice practical sessions to provide opportunities for troubleshooting and improving techniques.

The ‘Academic and Digital Literacies’ module provides formative assessment opportunities through group discussions and reflective logs. Tasks include reports where you analyse sources and critique them, applying cognitive skills integral to academic enquiry. The feedback from these activities aims to build your skills in researching, analysing and synthesising information.

‘Systems Management’ makes use of supported practical sessions where formative feedback can be given verbally to improve your practical techniques. For the coursework element of these modules, draft tasks related to coursework reports will be set helping you to improve your technique and interpretation of underpinning knowledge in real-world scenarios.

‘Network Programming and Scripting Concepts’ will initially have draft written and design tasks for theoretical elements to enable opportunities for written and/or verbal feedback. For the programming elements there will be supported workshops where issues with debugging techniques and problem solving can be aided with through small demonstrations or discussions of potential techniques to enhance your practice.

‘Network Disaster Recovery’ will enable formative feedback opportunities through setting disaster recovery planning task related to case studies. The database design and implementation aspect of the module will set formative tasks for providing designs and server links so that aspects of the implementation can be improved upon.

‘Introduction to Systems Security’ includes practical activities in sessions that are supported by verbal feedback to aid in troubleshooting and improving your techniques where links to underpinning knowledge are established. This module includes research and development of a security strategy and so formative tasks will be set to draft key elements of this, providing opportunities for you to improve.

Summative (Graded) Assessment

In 'Network Principles' and 'Introduction to Routing and Switching' there are timed practical sessions, online multiple choice exams and report based case studies where network equipment is specified and justified as well as designs for network infrastructure and research into core networking concepts. The 'Network Principles' module integrates the Cisco End of Chapter quizzes as part of the summative component; these are then used throughout the other Cisco embedded modules as formative tasks.

'Network Programming and Scripting Concepts' includes two pieces of coursework. The first will focus on theoretical concepts and where scripting tasks would be appropriate to increase efficiency for network professionals and also design tasks for a small-scale program. The second assignment will include developing a network-based program according to the design, testing and evaluating it.

The 'Network Disaster Recovery' module includes a large coursework element; the first assessment includes disaster recovery planning linked to a real-world scenario to be justified based on referenced evidence. The second coursework assessment includes the design, implementation, backup and transfer of a database with choices made requiring justification based on core database principles. There is a written exam in this module which will revisit concepts from different lenses and applied to different situations; the placement of this exam in the programme also aids in preparing you for exams in later levels of the programme which are a larger weighting of the module assessment.

'Introduction to Systems Security' will include practical activities embedded in larger coursework-based assessments to reinforce the links between practical techniques and underpinning concepts with a range of analysis techniques assessed. Comparisons and contrast of a range of reliable sources is also emphasised to base judgments upon.

YEAR 2 (LEVEL 5)

Formative Assessment

'Work Based / Placement Learning' will include reflective tasks throughout although some will count towards the summative assessment of the module. Other formative assessment activities include writing CVs and PDP to develop your employability skills.

'Project Management' will include as part of the formative assessment tasks draft plans, draft documentation (such as Risk Assessments, PID) and tasks based on case studies with a view improving your approaches to planning, documentation, judgment and consideration of legal, social, ethical and economic impacts.

'Virtualisation and Cloud Computing' includes practical activities in sessions that are supported by verbal feedback to aid in troubleshooting and improving your techniques where links to underpinning knowledge are established. In this module the practicals will have several 'mock' sessions beforehand to allow you to hone you skills prior to summative assessment. Tasks will be set based on elements of the coursework including writing up research into evolving cloud technologies and comparing different cloud solutions.

'Cyber Security and Process Management' is a largely theoretical module and so therefore there will be class tasks based on case studies and professional frameworks from which to receive verbal and/or written feedback. Lecturer-led class discussions will enable you to share different approaches with other students to topics whilst providing opportunities to clarify and challenge assumptions. There will be revision sessions with direct questioning / mock exam questions on which verbal and/or written feedback can be provided.

'Database and Web Security' and 'Data Evidence and Recovery' initially include theoretical

concepts and then a larger practical focus. Exploration of case studies, reflection on blended learning resources and lecturer-led discussions will provide opportunities for verbal and/or written feedback. Supported workshops for practical tasks will give you opportunities to practice the skills and receive feedback to reinforce concepts and refine techniques.

Summative (Graded) Assessment

'Work Based / Placement Learning' will include a work placement negotiated with an employer in industry and also comprise several reflective logs that link practice in modules to experience in the workplace and resolving where theoretical and practical skills are utilised in this environment. This will also include their experiences of developing as a professional and building towards their career goals. A second assessment will include a poster presentation reflecting upon the experience as a whole. The summative assessment for this module reinforces reflection, employability and transferrable skills with the poster presentation also preparing you for the Level 6 dissertation module.

'Project Management' has a coursework element that involves the planning and management of a networking based project including completion of all relevant documentation, justifications for choices made based on established methodologies and good practice in the profession. Critical analysis and judgement is emphasised in the assessment of the coursework. There is also an examination component which revisits core concepts from different angles and applies problem-solving skills to particular scenarios.

'Cyber Security Process Management' includes an in-depth report into Security Information Management that will explore concepts, definitions frameworks and techniques of information assurance, information security, threat modelling and risk management in the context of organisations. The written examination will cover roles, responsibilities, security policies, procedures, legal frameworks and security development lifecycles.

'Database and Web Security' and 'Data Evidence and Recovery' include a written piece of coursework and a larger piece which embeds practical elements. In 'Database and Web Security' the piece will focus on architectural concepts and trends in vulnerabilities and security mechanisms; the second piece will include a small-scale development to apply configuration and development techniques which guard against vulnerabilities with testing to ensure this. In 'Data and Evidence Recovery' the first piece will focus on technical fundamentals of data recovery and legal responsibilities in recovering evidence; the second piece will include the selection of a suitable methodology to recover data in a range of given contexts.

'Virtualisation and Cloud Computing' includes two timed practical assessments that focus on the deployment, configuration and testing of alternative virtualised solutions. The coursework element will examine wider issues and trends in cloud computing and implications this will have for network managers, comparing, contrasting and evaluating a wide range of reliable sources.

YEAR 3 (LEVEL 6)

Formative Assessment

'Cyber Ethics and Law' includes formative assessment tasks that rely upon your contributions to the class and your own research building your self-management and critical skills. This will include applying ethical principles to recent news articles and presenting judgements through seminars, discussions and written activities. Drafts on the summative essays will form part of the formative assessments enabling you to improve your writing, being more critical and concise. You will also undertake revision tasks revisiting principles and applying them to different cases to prepare you for the written exam.

'Distributed Systems' will include practical tasks where you will practice coding and debugging a prototype small scale program to demonstrate key concepts. In these sessions you will have

opportunities to be supported through feedback and help with debugging as well as discussing the links to the broader theoretical concepts. You will also be expected to research emerging technologies and core concepts in this subject area using academic papers to share with the class in discussions and build a shared understanding of the topics under discussion. There will also be opportunities to submit draft tasks related to the summative coursework submission enabling you to improve your writing and academic approach.

'Corporate Network Strategies' includes group tasks based on case studies to present to the class and provide opportunities for discussion based feedback to occur, questioning rationale, assessing where critical judgement has taken place and considering the approaches taken. Draft tasks based on the coursework will also be set helping you to improve prior to the exam.

'Cryptography and Cyber Security Trends' will include discussions based on your own research into topics related to the module content and the focus of discussions can be guided by them. There will be supported workshops for the small practical element where an encryption algorithm is produced which will enable feedback to be given on approaches. Draft tasks related to the written coursework and examination topics will be set to enable verbal and/or written feedback to be given.

The 'Dissertation' has a number of formative points throughout the year including proposal, ethical approval, project plan, literature review drafts, methodology drafts, design drafts, data analysis tasks, progress report and online reflective logs. Formative tasks are set every week according to a scheme of work that applies across Computing programmes and every two weeks this is recorded so that Personal Tutors can monitor progress and provide support where necessary.

Summative (Graded) Assessment

'Cyber Ethics and Law' includes multiple essays applying ethical principles to case studies and considering relevant legislative constraints and social impacts of evolving technologies. The exam revisits these principles and applies them to different contexts.

'Distributed Systems' includes the development of a small scale prototype to illustrate the importance of middleware and external data representation forming the basis for critical reflection on development and comparing this to the wider literature. The second assessment is a longer form investigative report which examines other aspects of distributed systems with an emphasis on exploring such topics in significant depth.

'Corporate Network Strategies' coursework involves the formulation of a corporate strategy which considers alignment of IT with other organisational operations, integrating a wide range of frameworks, theories and approaches with an emphasis on exercising critical judgement. The exam revisits these underpinning concepts from different angles.

'Cryptography and Cyber Security Trends' includes two written pieces of coursework. The first one examines cryptography in-depth and includes the writing of an encryption algorithm. The second piece is where Cyber Security trends are analysed and projections made for evolving threats / practices / technologies. The examination revisits concepts from the first two assignments from different lenses.

The 'Dissertation' summative assessment breakdown (to be taken as one whole assessment) is:

- Self-Management (15%)
- Dissertation Report (40%)
- Implementation / Development Work Done (35%)
- Poster / Demonstration (10%)

The overall summative piece will be blind cross-marked to ensure that the grade reached is an accurate reflection of your performance. Where an agreement cannot be reached then the Dissertation Co-ordinator will arbitrate to reach a final grade.

Programme Delivery: Work Based and Placement Learning

During the Foundation Degree you are expected to complete a minimum of approximately 100 hours of work placement. You are encouraged to secure these placements yourself through seeking out employers within the sector and through interview, applications or negotiation ascertain what your responsibilities will be and how they will be supported. It is expected that your placement has a direct relationship to the course content and so therefore you need to keep the academic staff aware of your intentions with regards potential placements. There are also legal requirements that must be met by employers including insurance and health and safety procedures; the Work Placement Co-ordinator will visit employers to ensure that the required information is in place. Periodically, the Work Placement Co-ordinator will check your progress with the employer.

A timetabled module on the second year of the programme will include delivery on aspects of professionalism and employability such as CV writing, Codes of Conduct, relevant legislation and interview techniques. In addition to these activities you are expected to maintain a digital log of your placement which will log hours, reflect upon the skills and techniques you have applied, how they relate to the course content and also planning for future graduate employment.

The tutorial sessions towards the end of the first year will provide you with more information in order to prepare you to seek out your placements as sometimes these can be completed in the summer break. Also, some placements may require DSB checks and staff can aid you with the completion of the required forms.

If you have difficulty securing a work placement, the Work Placement Co-ordinator maintains contacts with local employers and will work with you to be placed. If a placement cannot be located, a live employer related project will be undertaken for the required hours. It should be noted however that students who have shown the initiative in securing placements in areas of their interest have gone on to be successfully employed graduates with these and similar organisations.

The work placement elements of the course will have occurred on the pre-requisite FdSc. Network Engineering (Cyber Security).