Programme specification

(Notes on how to complete this template are provide in Annexe 3)

1. Overview/ factual information

Programme/award title(s)	Foundation Degree in Cyber Security with Cloud and Network Infrastructure
Teaching Institution	Belfast Metropolitan College
Awarding Institution	The Open University (OU)
Date of first OU validation	April 2018
Date of latest OU (re)validation	Nov 2022
Next revalidation	2027
Credit points for the award	240
UCAS Code	N/A
HECoS Code	100376
LDCS Code (FE Colleges)	N/A
Programme start date and cycle of starts if appropriate.	September 2023
Underpinning QAA subject benchmark(s)	• QAA Computing – March 2022 • CSE C2017 - CyberSecurity • IT 2017 – Information Technology
Other external and internal reference points used to inform programme outcomes. For apprenticeships, the standard or framework against which it will be delivered.	N/A
Professional/statutory recognition	N/A
For apprenticeships fully or partially integrated Assessment.	N/A
Mode(s) of Study (PT, FT, DL, Mix of DL & Face-to-Face) Apprenticeship	FT and PT
Duration of the programme for each mode of study	FT (2 year) and PT (2 ½ years)
Dual accreditation (if applicable)	N/A
Date of production/Revision of this specification	30/01/2023

Please note: This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided.

More detailed information on the learning outcomes, content, and teaching, learning and assessment methods of each module can be found in student module guide(s) and the students handbook.

The accuracy of the information contained in this document is reviewed by the University and may be verified by the Quality Assurance Agency for Higher Education.

Educational aims and objectives

Belfast Metropolitan College (the College) was established in 2007 following the merger of Belfast Institute of Further and Higher Education and Castlereagh College. The College has four sites across Belfast where it delivers higher education. The College delivers higher education across more than 30 subject areas in partnership with a number of universities (awarding bodies) including The Open University, Queen's University, Ulster University and the University of Dundee. The College runs a number of higher national diplomas and certificates in conjunction with Pearson and delivers a number of higher education professional and vocational courses with professional awarding organisations. The College also offers higher level apprenticeships in; cyber security and with cloud and network infrastructure, software and cloud development with data analysis, civil engineering and accounting.

The College's vision is to be a world class college that nurtures the talent and ambition of the City of Belfast and beyond. Its mission is to make a fundamental impact on the economic and social success of the city of Belfast and beyond by equipping its people, employers and communities with the education and skills for work and is supported by four strategic aims and four core values. The College works to meet its strategic aims through collaboration and membership of cross sector working groups and Northern Ireland specific, national and international college forums and groups.

The college currently offers full time and part time HE programmes in association with 4 university partners and 10 awarding bodies. In 2018-19 The college enrolled 2,698 learners onto HE programmes; 1,280 on to part time programmes and 1,444 onto full-time programmes. This is the largest HE in FE provision across the six FE colleges in Northern Ireland and the College is proud to have achieved its HE target and this demonstrates once again that demand for HE places exists in Belfast.

Since this Foundation Degree was validated there have been over 465 full time enrolments, not including the ever growing higher level apprenticeship programmes linked to this foundation degree. The Level 6 BSc (Hons) Top Up in Cyber Security and Networking Infrastructure validated in 2021 allows for an excellent progression route for successfully completing students. 47% of graduated students have already articulated to the Level 6 Top Up. Other articulation routes are: -

- Students are able to enrol on an Open University Top Up Degree IT offered through the Open University and complete four Level 6 modules.
- Students are able to enrol on year 3 IT programme at Napier University or Ravensbourne University.

Other possible articulation routes are: -

- Students can apply for Level 6 courses at the other two local Universities (Ulster University or Queens University) but will only gain entry onto to year 1 or year 2 (under consideration with distinctions in all Level 4 and Level 5 modules).
- Other UK Universities that the College is currently exploring articulation agreements with.

2.4 List of all exit awards
• Certificate in Higher Education in Cyber Security with Cloud and Network Infrastructure • Foundation Degree in Cyber Security with Cloud and Network Infrastructure

3. Programme structure and learning outcomes

(The structure for any part-time delivery should be presented separately in this section.)

Programme Structure - LEVEL 4					
Compulsory modules	**Credit points**	**Optional modules**	**Credit points**	**Is module compensatable?**	**Semester runs in**
Introduction to Networks	20			Yes	2
Host Security	20			Yes	2
Programming and Scripting	20			Yes	1
Cloud and Cyber Security Fundamentals	20			Yes	1
Mathematics for Computing	20			Yes	1
System Penetration Testing	20			Yes	2

Intended learning outcomes at Level 4 are listed below:

3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
A1: Appreciate and demonstrate through practice the fundamentals of cyber security. **A2**: Appreciate the theory and practice of a range of computer networking hardware and network operating systems. **A3**: Professional considerations: recognise the professional, economic, social, environmental, moral and ethical issues involved in the sustainable exploitation of computer. technology and be guided by the adoption of appropriate professional, ethical and legal practices. **A4**: Modelling: use such knowledge and understanding in the modelling and design of computer based systems. **A5**: Recognise a network engineering approach to the design and deployment of secure infrastructure solutions.	• Teaching and Learning Methods: Lectures, tutor directed tutorials, practical sessions, student led seminars and use of the College's Virtual Learning Environment. • Assessment Methods: Coursework related to assignments, case studies and projects, written unseen examinations, open book assessments, practical examination/observation and project reports.

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
B1: Specify and design computing security solutions to agreed standards. **B2**: Computational thinking including its relevance to everyday life. **B3**: Evaluate and test: explain the extent to which a computer based system meets the criteria defined for its current use and future development. **B4**: Discuss relevant modern business practices. **B5**: Relate professional, legal, moral and ethical issues to cyber security and infrastructure disciplines.	• Teaching and Learning Methods: Lectures, tutor directed tutorials, supervised practical sessions, student led seminars and use of the College's Virtual Learning Environment. • Assessment Methods: Coursework related to assignments, case studies and projects, written unseen examinations, open book assessments, presentations, practical examination/observation, project and placement reports. • Application and use of online virtual labs that enable students to construct real life scenarios to experiment and test out practical approaches to simulate advanced network configurations.

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1: The ability to specify and design reliable, secure and usable computer based systems. **C2**: Apply best practice processes, techniques and tools for the development and documentation of security, network design and risk management.	• Teaching and Learning Methods: Lectures, tutor directed tutorials, student led seminars, supervised practical sessions and self directed learning employing study packs and use of the College's Virtual Learning Environment.

3C. Practical and professional skills	
C3: Communicate technical information to technical, management, user and academic audiences. **C4**: Utilise computer and networking equipment effectively, based on an understanding of its hardware and software elements. **C5**: Assess problem solving using case studies on the economic issues, which influence organisations in an industrial context. **C6**: Develop effective solutions to practical problems individually and as a member of a team.	• Assessment Methods: Coursework related to assignments, case studies and projects, written unseen examinations, open book assessments, presentations, practical examination/observation, project and placement reports. • Application and use of online virtual labs that enable students to construct real life scenarios to experiment and test out practical approaches to simulate advanced network configurations. • Site visits to organisation and companies to reflect on industry standards, procedures, best practice and current trends. • Use of work based learning unit and case studies to build on knowledge and apply theoretical concepts and practical skills to real life situations. • Employ case studies in online virtual laboratories to test out advanced network security concepts.

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
D1: Students are expected to develop a wide range of generic skills to ensure they become effective in the workplace, to the benefit of themselves, their employer and the wider economy. **D2**: The ability to construct well argued and grammatically correct documents and communicate these effectively, using a range of media and with a variety of audiences. **D3**: Team working and management; the ability to recognise and make best use of the skills and knowledge of individuals to collaborate. To be able to identify problems and desired outcomes and negotiate to mutually acceptable conclusions. To understand the role of a leader in setting direction and taking responsibility for actions and decisions. **D4**: Self management; self awareness and reflection, goal setting and action planning, independence and adaptability, acting on initiative, innovation and creativity. The ability to work unsupervised, plan effectively and meet deadlines and respond readily to changing situations and priorities. **D5**: Interaction; reflection and communication, the ability to succinctly present rational and reasoned arguments that address a given problem or opportunity, to a range of audiences (orally, electronically or in writing).	• Teaching and Learning Methods: Lectures, tutorials, practical sessions and Work-based Learning. • Assessment Methods: Placement report assessment, written unseen examinations, open book assessments, presentations and coursework.

Exit award Level 4 is a Certificate of Higher Education in Cyber Security with Cloud and Network Infrastructure

Programme Structure - LEVEL 5					
Compulsory modules	**Credit points**	**Optional modules**	**Credit points**	**Is module compensatable?**	**Semester runs in**
Cloud Security	20			Yes	1
Incident Management	20			Yes	1
Work based Learning	40			No	2
Cloud Infrastructure	20			Yes	1
Implementation of Cyber Security	20			Yes	1

Intended learning outcomes at Level 5 are listed below:

3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
A1: Appreciate in some depth and demonstrate through practice knowledge of cyber security. **A2**: Appreciate the theory and practice of a range of computer networking hardware and network operating systems. **A3**: Professional considerations: recognise the professional, economic, social, environmental, moral and ethical issues involved in the sustainable exploitation of computer technology and be guided by the adoption of appropriate professional, ethical and legal practices.	• Teaching and Learning Methods: Lectures, tutor directed tutorials, practical sessions, student led seminars and use of the College's Virtual Learning Environment. • Assessment Methods: Coursework related to assignments, case studies and projects, written unseen examinations, open book assessments, practical examination/observation and project reports.

3A. Knowledge and understanding	
A4: Modelling; use such knowledge and understanding in the modelling and design of computer based systems for the purposes of comprehension, communication, prediction and the understanding of trade offs. **A5**: Apply a network engineering approach to the design and deployment of secure infrastructure solutions.	

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
B1: Specify, design and implement computing security solutions to agreed standards. **B2**: Computational thinking including its relevance to everyday life. **B3**: Critical evaluation and testing: analyse the extent to which a computer based system meets the criteria defined for its current use and future development. **B4**: Analyse and deploy relevant modern business practices. **B5**: Relate professional, legal, moral and ethical issues to cyber security and infrastructure disciplines.	• Teaching and Learning Methods; Lectures, tutor directed tutorials, supervised practical sessions, student led seminars and use of the College's Virtual Learning Environment. • Assessment Methods; Coursework related to assignments, case studies and projects, written unseen examinations, open book assessments, presentations, practical examination/observation, project and placement reports. • Application and use of online virtual labs that enable students to construct real life scenarios to experiment and test out practical approaches to simulate advanced network configurations.

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1: The ability to specify, design and construct reliable, secure and usable computer based systems. **C2**: Apply best practice processes, techniques and tools for the development and documentation of security, network design and risk management **C3**: Communicate technical information to technical, management, user and academic audiences. **C4**: Utilise computer and networking equipment effectively, based on an understanding of its hardware and software elements. **C5**: Assess and apply problem solving using case studies on the economic issues, which influence organisations in an industrial context. **C6**: Develop effective solutions to practical problems individually and as a member of a team.	• Teaching and Learning Methods; Lectures, tutor directed tutorials, student led seminars, supervised practical sessions and self directed learning employing study packs and use of the College's Virtual Learning Environment. • Assessment Methods; Coursework related to assignments, case studies and projects, written unseen examinations, open book assessments, presentations, practical examination/observation, project and placement reports. • Application and use of online virtual labs that enable students to construct real life scenarios to experiment and test out practical approaches to simulate advanced network configurations. • Site visits to organisation and companies to reflect on industry standards, procedures, best practice and current trends. • Use of work based learning unit and case studies to build on knowledge and apply theoretical concepts and practical skills to real life situations. • Employ case studies in online virtual laboratories to test out advanced network security concepts.

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
D1: Students are expected to develop a wide range of generic skills to ensure they become effective in the workplace, to the benefit of themselves, their employer and the wider economy. **D2**: The ability to construct well argued and grammatically correct documents and communicate these effectively, using a range of media and with a variety of audiences. **D3**: Team working and management; the ability to recognise and make best use of the skills and knowledge of individuals to collaborate. To be able to identify problems and desired outcomes and negotiate to mutually acceptable conclusions. To understand the role of a leader in setting direction and taking responsibility for actions and decisions. **D4**: Self management; self awareness and reflection, goal setting and action planning, independence and adaptability, acting on initiative, innovation and creativity. The ability to work unsupervised, plan effectively and meet deadlines, and respond readily to changing situations and priorities. **D5**: Interaction; reflection and communication; the ability to succinctly present rational and reasoned arguments that address a given problem or opportunity, to a range of audiences (orally, electronically or in writing).	• Teaching and Learning Methods; Lectures, tutorials, practical sessions and Work based Learning. • Assessment Methods; Placement report assessment, written unseen examinations, open book assessments, presentations and coursework.

3D. Key/transferable skills	
D6: Apply problem solving and critical thinking, making a case, numeracy and literacy, information literacy.	

Exit award at Level 5 is Foundation Degree in Cyber Security with Cloud and Network Infrastructure

Programme model

Programme Pathway	Years of Study	Semesters per year	Target group
Full Time	2 years	2	Aimed at full time students who will attend the college on a full-time basis.
Part Time	2 ½ years	2	Aimed at students enrolling on a Higher-Level Apprenticeship. These will be newly employed apprenticeships recruited by the organisation or company, employees with new responsibilities/duties in the area of Cloud and Applications Development or Level 3 Apprenticeships who are progressing to a Level 5 Higher Level Apprenticeship.

Annexe 1 - Curriculum map

This table indicates which study units assume responsibility for delivering (shaded) and assessing (✓) particular programme learning outcomes.

Level	Study module/unit	Programme outcomes																			
		A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	D5
4	Introduction to Networks	✓	✓		✓	✓	✓		✓	✓		✓	✓		✓		✓		✓	✓		✓
	Host Security	✓	✓	✓	✓	✓	✓	✓	✓				✓		✓			✓		✓	✓	
	Programming and Scripting	✓		✓		✓		✓	✓			✓	✓	✓		✓	✓	✓		✓	✓	
	Cloud and Cyber Security Fundamentals	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓				✓
	Mathematics for Computing	✓	✓			✓	✓	✓				✓		✓			✓			✓	✓	✓
	System Penetration Testing	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓

Level	Study module/unit	Programme outcomes																					
		A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	D5	D6
5	Cloud Security	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓				✓	
	Cloud Infrastructure	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓		
	Implementation of Cyber Security	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓
	Incident Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Work based Learning	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	