Programme Specification Template - Postgraduate

Please note:

- Guidance notes for staff or suggestions for the design and functionality of the database are in grey highlight. **Guidance notes should be deleted in the final version.**

SECTION A: CORE INFORMATION

1.	Name of programme:	Cybersecurity
2.	Award title:	MSc in Cybersecurity Post Graduate Diploma in Cybersecurity Post Graduate Certificate in Cybersecurity
3.	Programme linkage:	Is this part of group of linked programmes between which students can transfer at agreed points? (e.g. a group of programmes with a common set of taught modules) No
4.	Is the programme a top-up only?	No
5.	Level of award:	Level 7
6.	Awarding body:	University of Sunderland
7.	Department:	**Faculty of Computer Science**
8.	Programme Studies Board:	**Computing Postgraduate**
9.	Programme Leader:	**Dr David Nelson**

10. How and where can I study the programme?

Tick all boxes that apply

At Sunderland:	
Full-time on campus	X
Part-time on campus	X
As work-based learning full-time	
As work-based learning part-time	
As a full-time sandwich course	
As a part-time sandwich course	
By distance learning	

At the University of Sunderland London campus:	
Full-time on campus	
Part-time on campus	
As work-based learning full-time	
As work-based learning part-time	
As a full-time sandwich course	
As a part-time sandwich course	
By distance learning	

At a partner college:	
Full-time in the UK	
Part-time in the UK	
Full-time overseas	
Part-time overseas	
By distance learning	
As a full-time sandwich course in the UK	
As a part-time sandwich course in the UK	
As a full-time sandwich course overseas	
As a part-time sandwich course overseas	
As work-based learning full-time in the UK	
As work-based learning part-time overseas	
Other (please specify)	

Free text below to give further brief details (optional) – e.g. that the partner teaches the first part of the programme after which students progress to Sunderland. (Maximum 150 words)

11. How long does the programme take?

	Min number of years / months	Max number of years / months
Full-time	14 months	42 months
Part-time	24 months	72 months
Distance learning		
Work-based learning		

For start-dates please see the current edition of the Prospectus or contact the relevant department at the University. For start-dates for programmes delivered in a partner college, please contact the college.

SECTION B: FURTHER CORE INFORMATION

Use Outline Programme Proposal Form for ADC, for questions 12 to 23

24. Learning and teaching strategy

The general learning, teaching and assessment strategy used within this programme reflects the Faculty standard for postgraduate taught programmes and embraces the Faculty Learning and Teaching Plan. The fact that the MSc in Cybersecurity is dealing with graduates and educating them to Masters level means that the students are expected, and have the ability, to carry out a significant quantity of independent study. This may take the form of directed reading of research papers and advanced technical material, applied practical work utilising the tools and techniques appropriate to cybersecurity and the resolution of cybersecurity, resilience, business continuity and risk management and information security management problems.

The programme is designed to enable students to learn about the principles, theories, standards, policies and procedures associated with cybersecurity and to apply these in a series of practical, exciting and innovative ways. The programme encourages students to learn from leading researchers and practitioners in cybersecurity and as such lectures are underpinned with the opportunity to solve real world cybersecurity, resilience and continuity problems. Where possible these will be set from industrial and business contexts and case studies.

The case studies will be derived from collaborative partnerships from public and private sectors, for example from the (ISC)^2, Accenture, HPE, BT, PWC, SAGE, SRM, Net Defence, Sapphire, Sunderland City Council, Northumbria and Durham Police forces and the Cybersecurity Workforce Alliance, taking into account appropriate clearance, government agencies and organisations.

The intention is to give students an environment to:

- Explore, critically analyse and understand cybersecurity and related issues;
- Identify opportunities to utilise and apply cybersecurity principles and techniques in the design and implementation of robust systems;
- Develop strategies, policies and procedures to enhance cybersecurity;
- Prepare students for career development in the cybersecurity domain.

Negotiated learning is mainly used within the project module of this programme, but some of the assessment topics for modules (e.g. “Cybersecurity in Organisations”) will be negotiated between students and tutors. In the project module, the negotiation will centre on the terms of reference that the student wishes to propose. A central objective within the terms of reference of PROM02 will be the delivery of the product or artefact required by the client. However, the route by which this is achieved, and the topic and scope of the research that will interlink with it, are decided under negotiation between the student and supervisor (these decisions will be ratified during formal project reviews).

The cybersecurity provision is underpinned by strong collaboration with employers as indicated in the use of case studies above. The provision is further enhanced by the contribution from cybersecurity employers and external experts in a number of ways including, although not limited to, a series of guest lectures, master classes and seminars. The external input provides a range of different perspectives and helps to maintain the currency of the programme.

As indicated in sections 28 and 32 of this document, the MSc in Cybersecurity is heavily influenced by the research interests of the academics involved in the delivery of the modules. The MSc in Cybersecurity utilises the “research active curriculum” which enables MSc students to benefit from research in the Faculty and participate as researchers as an integral part of their studies.

25. Retention strategy

Support and guidance is offered to students through a comprehensive set of mechanisms in order to address retention. In addition to the details provided in the student support section retention on the MSc Cybersecurity programme will be addressed via student support and guidance, access to programme leader, module leaders, and personal tutors, during induction, via programme information (programme handbook), and access to student services and pastoral support.

All students have access to their Programme and Module Leaders as appointments can be made with staff. Students’ problems generally will be dealt with through the Programme Leader. The students also have representation on the Boards of Studies and the Staff Student Liaison Committees. Programme Leaders meet regularly with their tutees to take soundings and obtain feedback on various issues, and to talk to students individually to provide important academic guidance.

All students have access to a personal tutor. At postgraduate level the students’ personal tutor is their programme leader. Students can request to speak to their programme leader in confidence regarding any personal issues. In the case where a student, for example, would feel uncomfortable speaking with their programme leader (for example a female student may wish to speak with a female member of staff) then the programme leader will attempt to arrange for the student requests to be met as soon as possible.

All on-campus students have access to the University’s central support services including Counselling, Disability Service, Health and Well-being, Chaplaincy, financial support and advice, International Office and Careers and Employability Service. The Students’ Union provides an independent service which offers advice and support across the full range of personal and academic problems which students may encounter. Students wishing to lodge a complaint or an appeal can seek advice from the Students’ Union or from Academic Services. Full details of all these services can be found on the University’s web-site. Where appropriate, academic or support staff in the Faculty will sign-post students to these specialist services.

26. Any other information

The programme has been designed to incorporate the University’s principles and expectations of “inclusive programme design” in particular taking into account the requirements and availability of learning materials in hard copy / printed copy and online (taking into account W3C standards) – alternative formats will be signposted. All teaching and learning activities (see below) are designed to be inclusive by anticipating the most common problems that students with wide ranging levels of abilities may face. The teaching on the programme will embrace the principles of inclusive design for example by making whole module sets of material available in advance for students, use of vocabulary lists, facilitating recording of sessions, etc. The resources to be used on the programme comply with disability access requirements for University buildings – mainly in David Goldman Informatics Centre.

The Faculty of Computer Science utilises centralised disability support services to assess all students who require support on an individual basis. This is to ensure that appropriate support is identified and that a schedule is implemented to provide that support as necessary.

SECTION C: TEACHING AND LEARNING

27. What is the programme about?

The aims of the programme are to:

Provide you with advanced knowledge of cybersecurity topics and specialist areas including information security management; information risk management; implementation of secure systems; information assurance; incident (breach) management and business continuity.

Develop your research skills applicable to a career as a cybersecurity professional in industry or business or academia.

Stimulate your interest in the numerous applications of cybersecurity, including operational security management; risk management; information security; societal impact of cybersecurity; UXD and cybersecurity; artificial intelligence / machine learning in cybersecurity; cybersecurity and big data; and professional and ethical issues in cybersecurity.

28. What will I know or be able to do at the end of the programme? These should be brief bullet points for each sub-heading.

Learning Outcomes Postgraduate Certificate – Skills
By the end of this part of the programme successful students should know, understand or be able to do the following:

- **S1** Independently and objectively, critically review, consolidate and extend their knowledge to produce a systematic and coherent body of information in the context of cybersecurity
- **S2** Work independently and make objective decisions relating to complex cybersecurity problems and challenges
- **S3** Utilise and exploit the range of opportunities afforded by the application of cybersecurity principles, policies and procedures in specific contexts and settings

Learning Outcomes Postgraduate Certificate – Knowledge
By the end of this part of the programme successful students should know, understand or be able to do the following:

- **K1** undertake a thorough appraisal and understanding of a broad range of principles and practices in cybersecurity
- **K2** develop a thorough and critical understanding of key aspects of cybersecurity as an academic discipline
- **K3** critically apply appropriate research techniques with reference to studying cybersecurity
- **K4** understand at a conceptual level the theoretical underpinnings of cybersecurity

Learning Outcomes Postgraduate Diploma – Skills
By the end of this part of the programme successful students should know, understand or be able to do the following:

- **S4** design, build and evaluate complex ecosystems required in the development and implementation of cybersecurity applications using a wide range of methods, tools, techniques, languages and platforms
- **S5** create robust cybersecurity environments and integrate them with supporting architectures and infrastructures to produce reliable systems, networks, applications and procedures
- **S6** evaluate the risks associated with breaches in cybersecurity and the impact on business continuity, reputation and society in general
- **S7** apply creativity, innovation and enterprise to cybersecurity problems and opportunities

Learning Outcomes Postgraduate Diploma – Knowledge

By the end of this part of the programme successful students should know, understand or be able to do the following:

- **K5** have a critical awareness of the legal, professional, ethical, social and security issues associated with cybersecurity
- **K6** develop an appreciation of how architectures, infrastructure, operating systems, platforms and software interoperate to support cybersecurity environments, ecosystems and applications
- **K7** critically evaluate a range of processes, procedures and strategies, technologies and techniques utilised in cybersecurity

Learning Outcomes Masters – Skills

By the end of this part of the programme successful students should know, understand or be able to do the following:

- **S8** design and undertake independently, a major research project on a topic which relates to the forefront of the academic discipline of cybersecurity and reflect extensively and objectively on method, process and outcomes
- **S9** independently conduct research or advanced technical or professional activity on a project whose title is in the domain area of cybersecurity demonstrating self-direction and originality in tackling and solving problems, and critically evaluating sources
- **S10** deal with complex issues in cybersecurity both systematically and creatively, make informed judgements in the absence of complete data, and communicate their conclusions clearly to specialist and non-specialist audiences

Learning Outcomes Masters – Knowledge

By the end of this part of the programme successful students should know, understand or be able to do the following:

- **K8** critically apply management concepts and techniques, including the use of advanced tools for the management of cybersecurity research projects
- **K9** apply advanced knowledge in a highly specialised area, application or specialism in the discipline of cybersecurity, via an individual project

29. What will the programme consist of?

Taught postgraduate programmes generally consist of a number of taught modules leading to the award of a Postgraduate Certificate (60 credits) or Postgraduate Diploma (120 credits). A Masters qualification (180 credits) usually culminates in a major piece of independent work such as a project or dissertation. All modules are at postgraduate level (level 7 in the UK’s national scheme).

The summary below describes briefly what is contained in the programme. The programme structure, including a detailed list of modules, can be found in the programme regulations.

The Masters in Cybersecurity provides you with a thorough grounding in the creation of cybersecurity solutions for information security, systems security and network security, developing the skills to determine, establish and maintain cybersecurity infrastructures. You will have the opportunity to examine the underlying technologies of secure systems and develop a critical awareness of the inherent risks and related privacy issues of their use. You will have the opportunity to learn how to select the appropriate tools and techniques to address and manage concepts of risk; threats, vulnerabilities and potential attacks; and develop the technical and interpersonal skills to explain, apply and evaluate the concepts of trust and trustworthiness in cybersecurity contexts.

This programme will develop skills and knowledge to provide graduates with the confidence to apply cybersecurity tools and techniques; to be innovative in using cybersecurity skills; solve cybersecurity problems, identify breaches and attacks; create opportunities for information security management, risk management and business continuity; and to enable effective and efficient implementation of cybersecurity systems and infrastructures.

CETM30 Fundamentals of Cybersecurity. In this 30 credit module students will cover a range of governance and management topics which will enable students to determine, establish and maintain appropriate governance of, delivery of and creation of cybersecurity solutions for information security, systems security and network security. Students will be able to show a comprehensive understanding of the underlying technologies of secure systems and a critical awareness of the inherent risks and related privacy issues of their use in the cybersecurity environment by applying concepts such as the principle of least privilege, principle of separation of risk, defence in depth and secrecy. Students will learn to analyse the range of trade-offs in balancing the security properties of confidentiality, integrity and availability (CIA) and the usability demands of computer and information systems. They will have the opportunity to learn how to select the appropriate tools and techniques to address and manage concepts of risk, threats, vulnerabilities and potential attacks. Students will be able to explain, apply and evaluate the concepts of trust and trustworthiness in a cybersecurity context and explain and apply the issues associated with authentication, authorisation and access control.

CETM50 Technology Management for Organisations. The aim of the module is to critically discuss the management, organisation and use of cybersecurity and data science principles, policies and procedures in organisational settings. Students will have the opportunity to contextualise technology management ecosystems related to cybersecurity and data science depending on their field of interest and to examine the added value from technology as a business enabler. Students will also learn to apply the principles, policies and procedures of cybersecurity and data science to provide resilient and robust organisational solutions for secure and valuable information. Students will develop techniques and use tools that will enable them to undertake critical analysis of the challenges and opportunities of using cybersecurity to mitigate and manage risk to data and enable business continuity in the case of data breaches. They will also develop a critical understanding of governance, standards, audit, assurance and review in order to evaluate the challenges in managing technology.

CETM45 Cyber Resilience and Incident Response. Students will examine and evaluate the processes, procedures and protocols required to implement effectively secure and dependable systems. They will also consider cybersecurity in design and development using the concepts of secure design across a range of platforms and problem areas. Students will be introduced to topics such as applied cryptography, secure programming, defensive programming and their application in the design of secure systems. The student will learn how to model systems and define their security requirements using tools and languages for the formal specification of security protocols and systems and will consider enterprise applications and their security related applications. This module also provides individuals with the knowledge and skills to undertaken first response in cyber breach and associated incidents. Effective measures for securing evidential content in the wake of an event will be discussed and evaluated. Technical issues relating to breaches will be considered in order to evaluate effective response measures. Students will consider factors to contain breaches and limit the consequences emanating from these events. In addition, factors for mitigating risk will also be covered. Suitable procedures for notification of breaches will also be analyzed and the impact this may have on the organization and those directly affected by breach data loss, including surrounding legal context. Students will acquire the technical knowledge and skills to respond to breaches and implement proactive measures to potentially prevent their occurrence. All topics in the module will be considered taking into account professional, ethical, social and legal constructs.

CETM44 Cyber Security and User Experience Design. The module draws together two themes of cyber security and usability. These themes often appear orthogonal but their goals interact in complex ways that present trade-offs and challenges within software design. Helping students to understanding these trade-offs and challenges will is the focus of this module. The module will begin with an introduction to research challenges in the areas of usable security through a survey of past and recent research in usable cyber security. The module will then move on to examine, in detail, the nature of usability and the user experience, as it applies to cyber security, the impact of user psychology, user models, usage contents and usability evaluation techniques. After establishing this important contextual understanding the module will examine key challenges within usable cyber security and students will focus on of these challenges on which to focused within their assessed work.

Students who pass 60 credits CETM30 (Fundamentals in Cybersecurity – 30 credits) and one other module from the taught modules may be eligible for PG Cert. Students who pass an additional 60 credits from the taught modules are then eligible for a Postgraduate Diploma in Cybersecurity.

The final part of the MSc programme consists of a 60-credit project module **PROM02 Computing Master's Project**. In this module the student will develop a practical deliverable as well as investigate an area of academic research that informs the practical aspect of the project. Wherever possible the project will have a real client, who may come from either inside or outside of the institution and has a need for a real practical deliverable in the domain of cybersecurity.

PG Cert, PG Diploma and MSc requirements are summarised in the table below. Full detail of module name and assessment are available in the appendices.

Post Graduate Certificate in Cybersecurity	To obtain PG Certificate students need to pass CETM30 (30 credits)	Plus 1 30-credit module from CETM44, CETM45, CETM50
Post Graduate Diploma in Cybersecurity	To obtain PG Diploma students need to pass all taught modules, CETM30, CETM44, CETM45 and CETM50	

MSc in Cybersecurity	To obtain MSc students need to pass all modules for PG Diploma and also the 60 credit project module PROM02

30. How will I be taught? Modes of teaching and learning aligned with KIS – choose one or more

Scheduled teaching activities	X
Independent study	X
Placement	

Students will be given the opportunity to study the range of cybersecurity subjects using a variety of different teaching and learning approaches. The topics in the various modules will normally be introduced through a series of lectures led by academics who are active researchers in the subject matter and supported by guest lecturers from business and industry. The topics in the programme will normally include an examination of the theoretical aspects of the range of cybersecurity topics followed on with applied and practical activities.

Students will have the opportunity to examine and evaluate the environment of cybercrime and cyberthreat at individual, organisational and national level and as such the need and rationale for cybersecurity. Students will develop skills in a range of topics including security management, operational security management, risk management and threat evaluation, business resilience and continuity, development of policies and procedures in cybersecurity, and a range of tools and techniques in information security, systems security and network security.

All of the subjects and modules in the programme are aimed at developing cybersecurity professionals who understand the professional requirements and issues of the various roles in cybersecurity and are able to evaluate cybersecurity issues, challenges and opportunities taking into account legal, social and ethical considerations and requirements. The legal aspects of systems security, information security and information assurance are embedded throughout the programme. Ethical issues such as privacy protection, civil liberties, impact of cybersecurity on society, fixing or not fixing security vulnerabilities and disclosing or not disclosing system weaknesses are also addressed in the programme.

Students will have the opportunity to apply cybersecurity principles to real world security, threat and resilience challenges and problems. The programme will develop the students' research skills by encouraging them to participate in research into cybersecurity topics, deliver research seminars and present the findings of their research. Students will have the opportunity to explore the subjects in depth through guided independent study. A key approach to teaching and learning utilised in the MSc Cybersecurity is Problem Based Learning (PBL) (drawing on the pedagogic experience in the Faculty – currently there is a Higher Education Academy research project on using PBL in Cybersecurity being run in the Faculty of Computer Science giving the students the opportunity to examine cybersecurity subjects using innovative pedagogy).

The objective of the students-staff time in lectures is to introduce theories, concepts case studies and scenarios and to set milestones and learning goals, and make new ideas and concepts accessible to the students. These ideas are then followed up in tutorials and in the students' own time. Tutorials / seminars and laboratory activities are used within each module to provide support for lectures – giving students the opportunity to apply theoretical concepts to practical problems. Many of these practical problems will be set in collaboration with industrial and business partners to the University including $(ISC)^2$, Accenture, HPE, BT, PWC, SAGE, SRM, Net Defence, Sapphire, Sunderland City Council, Northumbria and Durham Police forces and the Cybersecurity Workforce Alliance. The prime objectives of tutorial time are to allow in-depth study of particular topics that have been introduced and also for practical exercises. As well as requiring a significant amount of individual study, the course also encourages group working. This is in recognition of the fact that a graduate of the course will normally be employed in environments where significant demands will be made upon his or her ability to co-operate and collaborate with others.

In addition students are expected, and have the ability, to carry out a significant quantity of independent study. Students will be supported in developing the skills to do this for example in CETM50, 'Technology Management for Organisations', and CETM30 'Cybersecurity Fundamentals'. This may take the form of directed reading of research papers and advanced technical material, research activities, or practical work on various software problems and packages. The level of independence increases throughout the programme culminating in the project module, PROM02, where students have the opportunity to demonstrate knowledge and skills from the taught modules and take them to a higher level.

As well as developing skills and abilities in the domain of cybersecurity, students will have the opportunity to develop Masters level skills, including, but not limited to: research skills (across all modules); gathering and using information; synthesising information/data; applying methodologies; applying concepts; creating new concepts/ideas/products; analysing and evaluating (technical aspects of cybersecurity; as well as the effectiveness of cybersecurity policies, procedures and strategies); critical reasoning, and information retrieval skills.

In the cybersecurity project students will have the opportunity to apply legal, ethical, social and professional issues (LSEPIs) when designing their project study and use LSEPIs to underpin the approach and all communication with the client. The professional body (British Computer Society) expectations are embedded throughout the programme – which will help with any students seeking to develop their careers by obtaining charted status (CITP or CEng).

Throughout the programme students will have the opportunity to develop the professional skills required for a career in cybersecurity including team working, problem solving, effective communications (written and verbal) and decision making. A common theme in the development of skills is the development of confidence to handle, manage and communicate in the cybersecurity domain. Students will be encouraged to develop their cybersecurity skills in such a way as to utilise the skills whilst maintaining confidentiality and integrity.

A list of the modules in the programme can be found in the Programme Regulations.

A summary of the types of teaching, learning and assessment in each module of the programme can be found in the Matrix of Modes of Teaching.

31. How will I be assessed and given feedback? Modes of assessment aligned with KIS: choose one or more.

Written examinations	
Coursework	X
Practical assessments	X

A summary of the types of teaching, learning and assessment in each module of the programme can be found in the Matrix of Modes of Teaching.

The generic assessment criteria which we use can be found here. Some programmes use subject-specific assessment criteria which are based on the generic ones.

This programme uses the Generic University Assessment Criteria	**YES**	**~~NO~~**
This programme uses the Subject Specific Assessment Criteria	**~~YES~~**	**NO**

The University regulations can be found here.

The assessment throughout this programme is a mixture of methods appropriate to the modules under study. Each assessed 30 credit module will typically have two assessments.

The students experience a diverse range of assessment strategies across the programme, enabling them to display various skills associated with Masters level learning. This will include research papers, creation of cybersecurity solutions (design, implementation, evaluation and maintenance), analysis of cybersecurity problems, threats and challenges, application of cybersecurity tools and techniques, creation of policies and procedures for cybersecurity, formal paper reviews, and presentations. The assessment strategies chosen within each module are appropriate to the content and style of delivery and have been further selected in order to provide a rich mixture of diverse assessment strategies while ensuring that the module aims and objectives can be accurately assessed.

Individual assignments include different forms of assessment strategies. The module CETM50 includes assessments where students undertake a research project presenting this as a poster or infograph. The module CETM44 Cybersecurity and User Experience Design also includes a research-focused assessment where students produce a critical review focused on one of the challenges in the toipic.

The module CETM44 Cybersecurity and User Experience Design also includes a practical assessment where students are required to design and implement an evaluation of a cyber security system with real users, presenting the results as an oral presentation. CETM50 Technology Management for Organisations also requires students to produce and present a strategic action plan for implementing a technology management strategy.

Every attempt is made to ensure that the assessments are based on real world problems and challenges, with assessment briefs being developed in collaboration with industrial and business partners where appropriate and as such have relevance to employers and help develop employability criteria for students. For example the module CETM30 Fundamentals of Cybersecurity includes two assessments both of which require students to analyse case studies.

The project module PROM02 encompasses a wide range of assessment styles whereby students produce a practical deliverable for a real client, a substantial and methodical research report which informs development of the practical deliverable and which must be relevant to the programme, a thorough evaluation of all stages of the project, and documentation evidencing project management and control of a substantial project.

The University aims to return marked assessments and feedback within 4 working weeks of the assignment submission date after internal moderation process have been completed. If this is not possible, students will be notified by the Module Leaders when the feedback is available and how it can be obtained.

The Academic Misconduct Regulations and associated guidance can be found here. It is the responsibility of students to ensure they are familiar with their responsibilities in regards to assessment and the implications of an allegation of academic misconduct.

Students should refer to the University Regulations for information on degree classifications.

32. Teaching, learning and assessment matrix

Matrix of modes of teaching, learning and assessment - MSc

NB. Not all option modules may be offered in any one academic year and will depend on the availability of staff and the priorities of the school. In addition, modules will usually need to be selected by a minimum number of students. Option modules may be available on more than one programme and the Programme Leaders will liaise with the Faculty Management Team to ensure there is a reasonable amount of choice in any given year.

Module	Code	Core / optional	Modes of T&L	Modes of Assessment	LO S1	LO S2	LO S3	LO S4	LO S5	LO S6	LO S7	LO S8	LO S9	LOS10
Cybersecurity Fundamentals	CETM30	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed	Taught Developed	Taught Developed		Taught Developed Assessed	Taught Developed
Technology Management for Organisations	CETM50	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught	Taught	Taught	Taught Developed Assessed	Taught	Taught Developed Assessed
Cyber Resilience and Incident Response	CETM45	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Developed	Developed	Taught Developed
Cybersecurity and User Experience Design	CETM44	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed		Taught Developed Assessed		Developed	Developed	Developed
Computing Masters Project	PROM02	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Developed	Developed	Developed	Developed Assessed	Developed Assessed	Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed

Module	Code	Core / optional	Modes of T&L	Modes of Assessment	LO K1	LO K2	LO K3	LO K4	LO K5	LO K6	LO K7	LO K8	LO K9
Cybersecurity Fundamentals	CETM30	Core	Lectures, Seminars,	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed	Taught Developed	Taught Developed	Taught Developed Assessed

			Tutorials, Self-study										
Technology Management for Organisations	CETM50	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Assessed	Developed Assessed	Taught Developed Assessed	Taught Developed Assessed			Taught Developed Assessed	Taught
Cyber Resilience and Incident Response	CETM45	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed	Taught Developed Assessed	Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Developed
Cybersecurity and User Experience Design	CETM44	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed		Taught Developed Assessed		Taught Developed		
Computing Master's Project	PROM02	Core	Lectures, Tutorials, Self Study	Coursework	Assessed	Developed	Taught Developed				Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed

Matrix of modes of teaching, learning and assessment – PG Diploma

NB. Not all option modules may be offered in any one academic year and will depend on the availability of staff and the priorities of the school. In addition, modules will usually need to be selected by a minimum number of students. Option modules may be available on more than one programme and the Programme Leaders will liaise with the Faculty Management Team to ensure there is a reasonable amount of choice in any given year.

Module	Code	Core / optional	Modes of T&L	Modes of Assessment	LO S1	LO S2	LO S3	LO S4	LO S5	LO S6	LO S7	LO S8	LO S9	LOS10
Cybersecurity Fundamentals	CETM30	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed	Taught Developed	Taught Developed		Taught Developed Assessed	Taught Developed
Technology Management for Organisations	CETM50	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught	Taught	Taught	Taught Developed Assessed	Taught	Taught Developed Assessed
Cyber Resilience and Incident Response	CETM45	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Developed	Developed	Taught Developed
Cybersecurity and User Experience Design	CETM44	Core	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed		Taught Developed Assessed		Developed	Developed	Developed

Module	Code	Core / optional	Modes of T&L	Modes of Assessment	LO K1	LO K2	LO K3	LO K4	LO K5	LO K6	LO K7	LO K8	LO K9
Cybersecurity Fundamentals	CETM30	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed	Taught Developed	Taught Developed	Taught Developed Assessed
Technology Management for Organisations	CETM50	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Assessed	Developed Assessed	Taught Developed Assessed	Taught Developed Assessed			Taught Developed Assessed	Taught
Cyber Resilience	CETM45	Core	Lectures, Seminars,	Coursework	Taught Developed	Taught Developed Assessed	Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Developed

and Incident Response			Tutorials, Self-study										
Cybersecurity and User Experience Design	CETM44	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed		Taught Developed Assessed		Taught Developed		

Matrix of modes of teaching, learning and assessment – PG Certificate

NB. Not all option modules may be offered in any one academic year and will depend on the availability of staff and the priorities of the school. In addition, modules will usually need to be selected by a minimum number of students. Option modules may be available on more than one programme and the Programme Leaders will liaise with the Faculty Management Team to ensure there is a reasonable amount of choice in any given year.

Module	Code	Core / optional	Modes of T&L	Modes of Assessment	LO S1	LO S2	LO S3	LO S4	LO S5	LO S6	LO S7	LO S8	LO S9	LOS10
Cybersecurity Fundamentals	CETM30	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed	Taught Developed	Taught Developed		Taught Developed Assessed	Taught Developed
Technology Management for Organisations	CETM50	Option	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught	Taught	Taught	Taught Developed Assessed	Taught	Taught Developed Assessed
Cyber Resilience and Incident Response	CETM45	Option	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Developed	Developed	Taught Developed
Cybersecurity and User Experience Design	CETM44	Option	Lectures, Seminars, Tutorials, Self Study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed		Taught Developed Assessed		Developed	Developed	Developed

Module	Code	Core / optional	Modes of T&L	Modes of Assessment	LO K1	LO K2	LO K3	LO K4	LO K5	LO K6	LO K7	LO K8	LO K9
Cybersecurity Fundamentals	CETM30	Core	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Taught Developed	Taught Developed	Taught Developed	Taught Developed Assessed
Technology Management for Organisations	CETM50	Option	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Assessed	Developed Assessed	Taught Developed Assessed	Taught Developed Assessed			Taught Developed Assessed	Taught
Cyber Resilience	CETM45	Option	Lectures, Seminars,	Coursework	Taught Developed	Taught Developed Assessed	Developed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed	Taught Developed	Developed

and Incident Response			Tutorials, Self-study										
Cybersecurity and User Experience Design	CETM44	Option	Lectures, Seminars, Tutorials, Self-study	Coursework	Taught Developed Assessed	Taught Developed Assessed	Taught Developed Assessed		Taught Developed Assessed		Taught Developed		

*Indicates a compulsory module which must be successfully passed for progression to further modules or to the next academic year of study

33. How does research influence the programme?

The Faculty of Computer Science is committed to the close coupling of research and teaching activities so that our research underpins the teaching we deliver. Research active staff are involved in the delivery of teaching across the complete range of our programmes. We actively map teaching teams to modules based on the relevance of their current activities and previous experience. The resulting cross-fertilisation of research and teaching means that our modules remain current in the rapidly developing field of cybersecurity.

The MSc programme in Cybersecurity is heavily influenced by the research interests of the academics involved in the delivery of the modules. All of the academics who are designated module leaders were returned in the most recent REF. Academic expertise in cybersecurity, digital forensics, information governance, big data, UXD, visualisation, machine learning, and network systems are embedded throughout the modules on the programme and underpin the learning outcomes of the MSc. Current research projects will be utilised to provide case studies and examples in the research active curriculum. Research specialisms and interests from colleagues in the faculty teaching on the programme include (but are not limited to): novel techniques for managing and discovering knowledge in cybersecurity; using cybersecurity to counter cybercrime and cyber-attacks; information security management; development of policies and procedures for cybersecurity; use of digital forensics to analyse security breaches; and UXD in cybersecurity. Examples of current projects include implementation of Cyber Essentials; raising employer and employee awareness in cybersecurity; development of cybersecurity policies and procedures in SMEs; gender issues in cybersecurity; identification of breaches using forensic techniques, evaluation of CISP; and pedagogic research looking at PBL in cybersecurity.

The MSc in Cybersecurity is heavily influenced by research both in terms of inclusion of research interests of academic staff and collaborative projects with industrial partners. The Faculty has a strong track record of Knowledge Transfer Partnerships as a means of formalising applied research.

Cybersecurity is one of the key research strands in the Faculty of Computer Science (along with Data Science, AI/Machine Learning, HCI/UXD and pedagogy in Computer Science) and as such has an active research group which includes 2 professors and 6 active researchers. Colleagues in the Faculty are involved in a number of collaborative projects with public and private business and industry. Students will have the opportunity to engage with the research projects.

Colleagues in the Faculty are involved in a number of external cybersecurity activities and organisations including work with DYNAMO North East, CyberNorth, North East Fraud Forum, $(ISC)^2$, and national standards development. Experience from participation and collaboration with these groups will be integrated into the curriculum providing examples and case studies as well as informing the curriculum.

We have a proud history of direct involvement from our students within our research activities. Masters projects are actively sourced from research areas in the Faculty and the University and recent publications have featured project work undertaken by students who have been included as named authors. Students have the opportunity to develop their research skills in a number of ways including as researchers through student led seminars, applying research (PROM01) and becoming part of the research community in the Faculty. Students will have the opportunity to participate in the Faculty's Research Seminar Series where one of the most active strands of the series focuses on cybersecurity.

SECTION D EMPLOYABILITY

34. How will the programme prepare me for employment?

The programme gives you the opportunity to develop advanced skills and knowledge which you can use in the future. Some postgraduate programmes are associated with a particular career path but most skills can be applied to a range of employment situations. The skills which this programme is designed to develop are listed below.

Work with CyberNorth, DYNAMO North East and individual employers including, BT, PWC, Net Defence, HPE, Sapphire and SRM indicate there are local, national and international skills gaps in cybersecurity, and demand is likely to grow.

Colleagues from the Faculty have been members of a national project bringing together academics, industry providers, professional bodies and employers. One of the outputs from the project is a report from (ISC)^2 / CPHC "Cybersecurity Principles and Learning Outcomes". The findings in this report suggest there is significant demand for specialist cybersecurity graduates and currently there are a number of employability issues including;

- 6% of the cybersecurity workforce in the UK is under 30;
- by 2020 globally there will be a shortfall of 1.5 million cybersecurity jobs;
- in the UK there are currently 62% too few InfoSec professionals;
- less than 10% of cybersecurity professionals are female;
- 57% of employers can't find graduates with the right mix of cybersecurity skills.

In 2016 the Government has developed strategies for the employment of cybersecurity in the private, public and not for profit sectors, but also in the fight back against the attackers.

The programme is a blend of theory, research informed curriculum, applied practice and problem based learning which go together to address the employability needs and skills gap issues.

There is strong employer input to the curriculum design and the delivery of the modules – with employers being consulted on curriculum content and skills required for cybersecurity employment. Employers provide a valuable resource in terms of guest lectures, master classes and problem setting for the programme.

The growth of cyber threats to individuals, businesses, organisations and governments are increasing at an unprecedented rate. Feedback from employers suggest that there is a significant skills gap in cybersecurity – there is a need for skilled professionals to address the needs and requirements of the industry in designing, implementing and maintaining cybersecurity solutions. The MSc in Cybersecurity seeks to develop graduates who will become proficient cybersecurity professionals with the technical knowledge base and skills set to master the complex problems and complex requirements in cybersecurity. The programme will enable graduates to utilise the constantly changing and evolving modern technologies that continuously reshape the way digital interaction and communication takes place. Recent government reports such as ***UK Commission for Employment and Skills*** *(2013) suggests that the* digital sector will require nearly 300,000 new recruits by 2020 and one of the key findings in the report suggests that specialist demand will include "high level IT specialisms, such as IT Architects, Data and **Security** specialists".

The MSc Cybersecurity programme has been designed in collaboration with employers regionally and nationally, including (ISC)^2, Accenture, HPE, BT, PWC, SAGE, SRM, Net Defence, Sapphire, Sunderland City Council, Northumbria and Durham Police forces and the Cybersecurity Workforce Alliance. One of the primary motivations for developing the cybersecurity programme was to address the skills gap in cybersecurity in the region and in the UK. The programme learning outcomes, the content of the programme and the content and curriculum for each module has been designed in order to address the subject specific needs of employers. Each module has included a definition of the transferrable skills that are specifically developed in the individual modules. The transferable skills have been designed to enhance the employability of students.

The Faculty of Computer Science works closely with the University's central Careers and Employability Service to ensure that students have access to career opportunities, specialist talks and support and guidance for career development. For full time students there is a commitment to supporting students in their progression from education to work. For part time students support is given to help with career development and career progression. The Careers and Employability Service is located in the Gateway, an impressive, newly-renovated facility in the centre of the City Campus.

There are also opportunities for on-campus students outside your programme of study.
Where applicable add text about any extra-curricular activities or opportunities provided by the faculty / department to support students' general development, their integration as a cohort, career planning etc.

For information about other opportunities available to our students who study on campus, click here.

Additional opportunities to develop your experiences more widely will vary if you study at one of our partner colleges. For information about the extra-curricular activities available in any of our colleges please contact the college direct.

35. Particular features of the qualification. (optional)

This describes key features relevant to employability and will be reproduced in the HEAR. If any of the following features apply to all students who achieve this award, please describe them briefly below: placement, professional practice element, key programme specific regulations, professional body accreditation.
For example: "Graduates of this programme will have undertaken a minimum of 80 hours in professional practice. Completion of this programme entitles the graduate to Associate Membership of the Origami Council." (Maximum 150 words)

36. Professional statutory or regulatory body (PSRB) accreditation. Choose one of the following.

PSRB accreditation is not relevant to this programme	
PSRB accreditation is currently being sought for this programme	
This programme currently has PSRB accreditation	X

The programme is currently accredited until:

The implications of the accreditation not being renewed are:

Please see PSRB Renewal Process for information on the renewal process.

The relevant PSRB(s) is/are:

British Computer Society

The terms of the accreditation are as follows:

- Students must complete their programme of study within six years.
- Students must have completed the entire programme at the University of Sunderland.

The programme is recognised as:

Partially meeting the requirement for Chartered IT Professional

The programme is accredited dependent on

Successful completion of 180 masters credits

This depends upon successful completion of the programme.

Is membership of the PSRB dependent on further requirements? No

There are no programme-specific regulations relating to this award.

The modules to be studied	n/a
Pass-marks for some or all modules and/or parts (elements) of modules	n/a
Placement requirements	n/a
Attendance requirements	n/a
Professional practice requirements	n/a
Final or overall mark for the award	n/a
Other	n/a

Interim or exit awards are not accredited.

Free text for description which is not covered by the options above.

(Maximum 50 words)

Repeat if necessary for more than one PSRB

SECTION E: PROGRAMME STRUCTURE AND REGULATIONS

See Appendix 1.

SECTION F: ADMISSIONS, LEARNING ENVIRONMENT AND SUPPORT

40. What are the admissions requirements?

Entry point (delete those not required)	**Standard entry requirements**[1]	**Entry with advanced standing**[2]	**Other**[3]
Level 7 (Masters awards) – start of programme	An honours degree (2:2 or above) or equivalent in a computing or related non-computing discipline	Not applicable	Students who have 5 years relevant business or industry experience

	(mathematics, statistics, engineering)		
Level 7 (Masters awards) – after Certificate	Not applicable	Not applicable	
Level 7 (Masters awards) – after Diploma	Not applicable	Not applicable	

Applicants whose first language is other than English must fulfil the University's minimum language skills requirement through one of the accepted mechanisms.

The University's standard admissions requirements can be found in the university regulations. Programme-specific requirements which are in addition to those regulations are given below. (Maximum 100 words)

Can students enter with advanced standing?	**~~Yes~~**	**No**

The University has a process by which applicants whose experience to date already covers one or more modules of the programme they are applying for may seek Accreditation of Prior Learning (APL). Full details can be found here but if you think that this may be relevant to you, please contact the department which offers the programme you are interested in.

APL and APEL are not normally applied in this programme.

41. What kind of support and help will there be?

a. in the department:

The overall strategy for support and guidance is three-pronged: accessibility to staff and resources; provision of relevant and reliable information; and operation of a responsive system for managing problems as they arise.

Support and guidance is offered to students through a comprehensive set of mechanisms. All new students are given a week-long induction programme during which time they are exposed to various aspects of student academic life and much information on the University and its Services, the Faculty of Computer Science and their chosen programme of study. They are provided with programme information, talks by programme and module staff, library visits, talks by representatives from a number of important student services such as the International Office and the University language Scheme including English for Academic Purposes for students whose first language is not English.

All students have access to their Programme and Module Leaders as appointments can be made with staff. Students' problems generally will be dealt with through the Programme Leader. The students also have representation on the Boards of Studies and the Staff Student Consultative Committees. Programme Leaders meet regularly with their tutees to take soundings and obtain feedback on various issues, and to talk to students individually to provide important academic guidance.

Library facilities for students are provided across both campuses and offer an innovative learning environment, an electronic environment which offers access to online resources, the campus network and the Internet, and areas for group and individual study. A summary of the major features of the Web provision, which will be available to the students, is given below:

- complete staff list, telephone numbers, Email addresses and module responsibilities;
- complete list of Faculty of Computer Science programmes, modules with links to programme structures and module descriptors;
- generic student handbook including links to Faculty home pages, University sites e.g. Student Services, Careers, Information Services, Campus maps and various Faculty and University policy documents e.g. rules on infringement, the Modular Credit Scheme and Teaching & Learning policies;
- health & Safety advice;
- the use of Canvas (on-line learning environment) to act as a student support and feedback mechanism.

All students have access to a personal tutor. At postgraduate level the students' personal tutor is normally their programme leader. Students can request to speak to their programme leader in confidence regarding any personal issues. In the case where a student for example would feel uncomfortable speaking with their programme leader (for example a female student may wish to speak with a female member of staff) then the programme leader will attempt to arrange for the student requests to be met as soon as possible.

for careers guidance through the programme / department. (Maximum 500 words)

b. *in the university as a whole:*

The University provides a range of professional support services including wellbeing, counselling, disability support, and a Chaplaincy. Click on the links for further information.

c. *in a partner college:*

Please see the relevant college prospectus or website for details of student support if you are planning to study in one of our partner colleges.

42. What resources will I have access to?

On campus	X	In a partner college		By distance learning	

On campus

Tick all that apply

General Teaching and Learning Space	X
IT	X
Library	X
VLE	X
Laboratory	X
Studio	
Performance space	
Other specialist	
Technical resources	X

In terms of our teaching staff, the module leaders have been chosen with regard to their expertise in the subject area and in many cases they, and their teaching team, are working on relevant research and/or external engagement projects. This enables staff to practice research informed teaching thus providing students with an appreciation of relevant research themes, an idea of where and how the subject is developing in the future and, in many cases, "real world" case studies. External speakers are solicited from collaborating companies and our own recent graduates in order to provide students with access to relevant practitioners who can provide industrial context.

The list of module leaders involved in the delivery of this programme can be seen in Appendix 2.

The Faculty makes full use of the University's Virtual Learning Environment (Canvas) and our strategy is for every module and programme to have an online presence. Key features of our current Canvas provision include:

- complete staff list, telephone numbers, Email addresses and module responsibilities;
- complete list of Faculty modules with links to detailed module descriptors and, in many cases on-line learning resources;
- general student handbook including links to Faculty home pages, University sites e.g. Student Services, Careers and Employability Service, Information Services, Campus maps and various Faculty and University policy documents e.g. rules on cheating and collusion, the Modular Credit Scheme and Teaching & Learning policies;
- Faculty Programme/Module timetables;
- Faculty Standards;
- A Code of Conduct for Use of the Computing Terraces;
- Health and safety advice;
- Information about the Faculty's research activities.

Library facilities available at St Peters include a dedicated computing subject collection, a comprehensive range of electronic resources, open access areas for group and individual study, and dissertations / research working papers from the Faculty are also housed in the library.

Specialist Resources

All students in the Faculty are provided with access to one of the most modern and best equipped computing environments in the UK. The David Goldman Informatics Centre features an open plan area made up of terraces which contain nearly 250 workstations comprising PCs and MACs. The computers on the terraces are installed with all the necessary software packages required and are normally available to the students on an open access basis 7:00am until 9:00pm weekdays. 24 hour computing facilities are available at the Murray Library.

In support of independent study, students are provided access to the Internet for their smartphones, tablets and laptops via a university wide wireless network. A range of free software is also made available to students through volume licensing with partners such as Adobe, Symantec, Microsoft and Cisco.

The programme makes use of specialist hardware (including a 40 core grid computer, Dell R920 60 core processor, 1 G RAM & high capacity storage) and software resources for the MSc Cybersecurity programme. These will enable students to understand the relationship between hardware and software in cybersecurity management and the development of cybersecurity solutions. The cybersecurity programme and modules will utilise the specialist network security laboratories and the forensics / breach management laboratory.

The Enterprise Place is supported by the Sunderland Software City initiative and provides dedicated rooming and facilities to host entrepreneurial activities in Cybersecurity. Students with business ideas can become resident in Enterprise Place as they attempt to grow from ideas on how to exploit Cybersecurity opportunities to fully formed businesses.

Information about the University's facilities can be found here.

Please see the relevant college prospectus or website for details of college learning resources if you are planning to study in one of our partner colleges.

43. Are there any additional costs on top of the fees?

No, but all students buy some study materials such as books and provide their own basic study materials.	*X*
Yes (optional) All students buy some study materials such as books and provide their own basic study materials. In addition there are some are additional costs for optional activities associated with the programme (see below)	
Yes (essential) All students buy some study materials such as books and provide their own basic study materials. In addition there are some are essential additional costs associated with the programme (see below)	

44. How are student views represented?

All taught programmes in the University have student representatives for each programme who meet in a Student-Staff Liaison Committee (SSLC) where they can raise students' views and concerns. The Students' Union and the faculties together provide training for student representatives. SSLCs and focus groups are also used to obtain student feedback on plans for developing existing programmes and designing new ones. Feedback on your programme is obtained every year through module questionnaires and informs the annual review of your programme. Student representatives are also invited to attend Programme and Module Studies Boards which manage the delivery and development of programmes and modules. Faculty Academic Committee, also has student representation. This allows students to be involved in higher-level plans for teaching and learning. At university level on Students are represented on University level Committed by sabbatical officers who are the elected leaders of the Students' Union.

The University's student representation and feedback policy can be found here.

Every year we participate in the national Postgraduate Taught Experience Survey (PTES).

Programmes offered in partner colleges*:* If you are studying in one of our partner colleges the college will have its own mechanisms for obtaining student feedback. Some of these may be the same as those on-campus at the University but others may be different. You should ask your college for further information.

For distance learning operated from Sunderland: if you are studying by distance learning you will have slightly different arrangements from those used on campus. In particular you are likely to have virtual rather than physical meetings and discussions. However these arrangements should provide comparable opportunities for you to give feedback. Details are given below.

SECTION G: QUALITY MANAGEMENT

45. National subject benchmarks

The Quality Assurance Agency for Higher Education publishes benchmark statements which give guidance as to the skills and knowledge which graduates in various subjects and in certain types of degree are expected to have. They do not cover all subjects at postgraduate level but those which exist can be found at here.

Are there any benchmark statements for this programme?	**YES**	**~~NO~~**

The subject benchmark(s) for this programme is/are:

Masters Computing Benchmark

The programme development has also drawn heavily from the GCHQ Requirements for Masters programmes in Cybersecurity, available at https://www.ncsc.gov.uk/articles/gchq-degree-certification-call-new-applicants. Whilst the programme will seek accreditation from the BCS as the professional body for computing, the programme will also seek accreditation from GCHQ.

The QAA also publishes a Framework for Higher Education Qualifications (FHEQ) which defines the generic skills and abilities expected of students who have achieved awards at a given level and with which our programmes align. The FHEQ can be found here.

A table mapping the programme learning outcomes against the QAA benchmark for Computing Master's courses can be found in Appendix 4.

46. How are the quality and standards of the programme assured?

The programme is managed and quality assured through the University's standard processes. Programmes are overseen by Module and Programme Studies Boards which include student representatives. Each year each module leader provides a brief report on the delivery of the module, identifying strengths and areas for development, and the programme team reviews the programme as a whole. The purpose of this is to ensure that the programme is coherent and up-to-date, with suitable progression through the programme, and a good fit (alignment) between what is taught and how students learn and are assessed - the learning outcomes, content and types of teaching, learning and assessment. Student achievement, including progress through the programme and the way in which the final award is made, is kept under review. The programme review report is sent to the Programme Studies Board and the Faculty in turn reports issues to the University's Quality Management Sub-Committee (QMSC).

External examiners are appointed to oversee and advise on the assessment of the programme. They ensure that the standards of the programme are comparable with those of similar programmes elsewhere in the UK and are also involved in the assessment process to make sure that it is fair. They are invited to comment on proposed developments to the programme. Their reports are sent to the Deputy Vice-Chancellor (Academic) as well as to the Faculty so that issues of concern can be addressed.

All programmes are reviewed by the University on a six-yearly cycle to identify good practice and areas for enhancement. Programmes are revalidated through this review process. These reviews include at least one academic specialist in the subject area concerned from another UK university. Quality Assurance Agency (QAA) review reports for Sunderland can be found here.

Further information about our quality processes can be found here.

Please also complete and insert the SITS form.

See Appendix 2.

Appendix 1

PART B - PROGRAMME REGULATION/S

Name of programme: *Cybersecurity*
Title of final award: *MSc Cybersecurity*
Interim awards[1]: *Postgraduate Certificate in Cybersecurity, Postgraduate Diploma in Cybersecurity.*

Students who pass 60 credits (which must include 'Cybersecurity Fundamentals' CETM30) are eligible for a Postgraduate Certificate in Cybersecurity. Students who pass all the taught modules on the programme are eligible for a Postgraduate Diploma in Cybersecurity.

Accreditation: *MSc in Cybersecurity has initial accreditation by the BCS for the 2017 intake. The other awards are not accredited.*

University Regulation (please state the relevant University Regulation)**:** *4.2.1. The overall pass mark for each module is 40%. To pass a module a student must also have submitted work for each element of assessment.*

Regulations apply to students commencing their studies from (please state the date / intake that these regulations will apply to students for each Stage)**:**

Regulations apply to students	**Date the regulations apply**	**Intakes affected**
Stage 1		
Stage 2		
Stage 3		
Stage 4	September 2018	September 2018 onwards

Stage 4

Core modules:

	Code	Title	Credits
CERT PHASE	*CETM30*	*Fundamentals of Cybersecurity*	*30*
CERT/DIP PHASE	*CETM44*	*Cybersecurity and User Experience Design*	*30*
	CETM45	*Cyber Resilience and Incident Response*	*30*
	CETM50	*Technology Management for Organisations*	*30*
MASTERS PHASE	*PROM02*	*Computing Masters Project*	*60*

Optional Modules

None

Elective Modules

None

Progression Regulations

[1] Same as main award unless agreed otherwise at validation – eg to meet PSRB requirements

There are no programme-specific progression regulations[2]

[2] This will be the norm – university regulations apply

Appendix 2

Quality Handbook

SITS SUMMARY PROGRAMME/SHORT COURSE DETAILS

(Form to be completed electronically by the Faculty and forwarded to the Quality Support Officer supporting the Approval event, or sent to Planning & MI for faculty devolved processes before sending to Quality Support (with the exception of Short Courses and GRS))

This form is to be completed when a new programme has been validated and approved so that the programme codes and progression and awards rules can be set up in SITS. This also needs to be completed at periodic course review when there have been significant modifications to the course.

Please note that all details entered onto this form will go onto every student's record that is attached to this programme and it is therefore imperative that the information is correct.

1 Programme Details		
New/ Modification/Review: Please ensure the minor modification document is included	**Modification**	
Full Programme Title:	**MSc Cybersecurity**	
If replacement for existing course, specify title and course code:		
Qualification Aim: e.g. Foundation degree of Science, Bachelor of Arts (Honours)	Masters	
Qualification Level (NQF level):	7	
JACS 3.0 code JACS code = e.g. (V100) History, (I100) Computing Science, etc. See HESA Website https://www.hesa.ac.uk/jacs3	I100	
Is the programme Open or Closed: A course is defined as closed when specifically designed for a certain group of people and not also available to other suitably qualified candidates. It may be designed for a particular company however if the same course is also run for other suitably qualified candidates, not employed by the company, then the course is not closed.	Open	
Faculty and School:	Computer Science	Computer Science
Location of study: e.g. SAGE, Sunderland in London, Sunderland	Sunderland	
Last Date Registration (PBI) Number of days: The number of days after the start date of the course that it is possible for students to register onto it. It is also referred to as the migration date.	15	
Programme Leader:	Dr David Nelson	
Academic Team for the programme:	Postgraduate computing team	
Date of Approval/Modification/Review:	7th December 2016	
Date of next review (*QS to complete*):		

Accrediting Body or PSRB If yes please attach a completed PSRB form	Yes/~~No~~
Programme Specific Regulations If yes, please attach a completed Programme Specific Regulations form	~~Yes~~/No/~~Pending~~
Does this programme come under the Key Information Set return? If yes, please attach a completed KIS form	No
Is this an undergraduate programme whose primary (but not necessarily only) purpose is to improve the effectiveness of practitioners registered with a professional body? If yes, please specify which body: http://www.hefce.ac.uk/media/HEFCE,2014/Content/Pubs/2016/201622/HEFCE2016_22.pdf (Page 88, paragraph f) e.g. a short course aimed at registered nurses	~~Yes~~/No Professional Body:

Interim Awards

If a student does not achieve their qualification aim, what lower awards might they be entitled to, assuming they have the credits? The subject title for any lower level award should be given where this is different from the subject of the qualification aim.

	Interim Award Title	Credits Required	Interim Structure Please show mandatory requirements if applicable e.g. core module codes
1	PG Certificate in Cybersecurity	60	CETM30 and one from CETM33, CETM45, CETM50
2	PG Diploma in Cybersecurity	120	CETM30, CETM33, CETM45 and CETM50
3			

Combined Subjects Programmes only

Will the subject run as Major/Minor/Dual:	
Any subject(s) not permitted to be combined with this subject:	

2 Mode Of Attendance

01	Full-time *Full-time students are those expected to study for more than 24 weeks per year, for a minimum of 21 hours per week and are paying the full-time fee.*	Yes
02	Other Full-time *Students who attend full-time for a period less than 24 weeks per year*	
31	Part-time *Students who are expected to study for less than 21 hours per week.*	Yes
31	Part-time at Full-time Rate *Students who are studying full-time credits over part-time attendance*	

3 Admissions An admissions or MCR code will be created to allow student applications.	Tick appropriate

U	UCAS Universities and Colleges Admission Services *Required for full-time undergraduate programmes only.*	
D	Direct Entry *Required for FT, PT, PG and PGR, only where students will be admitted though the admissions teams or where the programme needs to be advertised on the web*	Yes
G	GTTR Graduate Teacher Training Registry *Education only, where applicable*	

4 Collaborative Provision	UK	
	Overseas	
Institution	Collaborative Model	Funding Arrangements

5a Course Block	
Full-time - Overall length of the programme in months:	14 months
Part-time - Overall length of the programme in months:	24 months
Does this course offer a sandwich placement? If **yes**, please indicate which programme year this placement is to take place.	~~Yes~~/No Programme Year:
Is this compulsory or optional?	Compulsory/Optional
Does this course offer a study abroad year out? If **yes**, please indicate which programme year this placement is to take place.	~~Yes~~/No Programme Year:
Is this compulsory or optional?	Compulsory/Optional

6 Major Source of Funding **Please note** this relates to funding for the programme and **not** individual students	
HEFCE Higher Education Funding Council for England	Yes
Skills Funding Agency/EFA/Degree Apprenticeship	
NCTL National College for Teaching and Leadership	
Wholly NHS Funded Partially NHS Funded Departments of Health/NHS/Social Care. ***For all Health funded programmes please indicate whether the programme is eligible for an NHS Bursary*** - Eligible for NHS Bursary Y/N	
Standard Fee If no then the Learning Resources Form should be attached	Yes/~~No~~
Other Funding:	

– Please Specify:

7 Education Programmes Only This section must be completed for any programmes marked above as 'NCTL' funded	
Teacher Training Identifier:	
Teacher Training Scope:	
Qualification Aim: QTS and academic award, QTS only, QTS by assessment only	

DETAILS SUPPLIED BY: …Dr David Nelson…………………………… DATE: ………………………..

Module List

Award, Route (if applicable) and Level	**New/Existing/ Modified Module (N/E/MM)**	Module Title	Module Code	Module Credit Value	Whether core or option	Must choose (i.e. designated option):	Assessment weighting – give % weight for *each assessment item*	Pre-/co-requisites	Module leader	Other comment (if required)	Date of Entry on SITS. N/MM only (After event)	JACS Code	Academic Team
Taught (Cert/Dip)	MM	**Fundamentals of Cybersecurity**	**CETM30**	**30**	**Core**		**001 Coursework 50%** **002 Coursework 50%**		**Prof. Alastair Irons**			**I100**	
	N	**Cybersecurity and User Experience Design**	**CETM44**	**30**	**Core**		**001 Coursework 50%** **002 Coursework 50%**		**Dr. Sharon McDonald**			**I140**	
	N	**Cyber Resilience and Incident Response**	**CETM45**	**30**	**Core**		**001 Coursework 50%** **002 Coursework 50%**		**Dr. Paolo Modesti**			**I100**	**Dr Paolo Modesti, Prof. Chris Bowerman**
	N	**Technology Management for Organisations**	**CETM50**	**30**	**Core**		**001 Coursework 40%** **002 Coursework 60%**		**Prof. Alastair Irons**			**I100**	

Masters	N	**Computing Master's Project**	**PROM02**	**60**	**Core**		**001 Coursework 10%** **002 Coursework 60%** **003 Viva + Coursework 30%**		**Dr. David Nelson**			**I100**	**Dr David Nelson, Dr Sharon McDonald**

APPENDIX 4 - Benchmark mapping – MSc Cybersecurity

The QAA benchmark specifies the threshold standard of achievement, i.e. the standard expected to be achieved by a student graduating with the award of a master's degree in computing. The threshold level specifies:

7.2 All students graduating with a master's degree in computing are expected to be able to have demonstrated:

1. a systematic understanding of the knowledge of the domain of their programme of study, with depth being achieved in particular areas, including both foundations and issues at the forefront of the discipline and/or professional practice in the discipline; this should include an understanding of the role of these in contributing to the effective design, implementation and usability of relevant computer-based systems
2. a comprehensive understanding, and a critical awareness of: the essential principles and practices of the domain of the programme of study as well as current research and/or advanced scholarship; current standards, processes, principles of quality and the most appropriate software technologies to support the specialism; the relevance of these to the discipline and/or professional practice in the discipline; and an ability to apply these
3. consistently produced work which applies to and is informed by research and/or practice at the forefront of the developments in the domain of the programme of study; this should demonstrate critical evaluation of aspects of the domain, including appropriate software support, the ability to recognise opportunities for software or hardware tool use as well as possible tool improvement, an understanding of the importance of usability and effectiveness in computer systems development, and generally the acquisition of well-developed concepts
4. understanding of the professional, legal, social and ethical framework within which they would have to operate as professionals in their area of study; this includes being familiar with and being able to explain significant applications associated with their programme of study and being able to undertake continuing professional development as a self-directed lifelong learner across the elements of the discipline
5. the ability to apply the principles and practices of the particular programme's domain in tackling a significant domain related activity; the solution should demonstrate a sound justification for the approach adopted as well as originality (including exploration and investigation) and a self-critical evaluation of effectiveness but also critical awareness of current problems and new insights, and a sense of vision about the direction of developments in aspects of the domain of the programme.

The tables below provide a mapping of the benchmark against the programme learning outcomes:

	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**
1	Y			Y	Y			Y		Y
2			Y	Y	Y	Y		Y	Y	
3	Y			Y			Y	Y	Y	
4		Y	Y			Y				
5			Y				Y	Y	Y	Y

	K1	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**	**K9**
1	Y	Y	Y	Y	Y	Y	Y		Y

2			Y	Y		Y	Y	Y	Y
3	Y	Y	Y					Y	Y
4					Y		Y		
5			Y					Y	Y