GLASGOW CALEDONIAN UNIVERSITY

Programme Specification Pro-forma (PSP)

1. GENERAL INFORMATION

1.	**Programme Title:**	MSc Cyber Security (GA)
2.	**Final Award:**	MSc Cyber Security
3.	**Exit Awards:**	PgC / PgD Cyber Security
4.	**Awarding Body:**	Glasgow Caledonian University
5.	**Approval Date:**	12 June 2018
6.	**School:**	School of Engineering and Built Environment
7.	**Host Department:**	Department of Computer, Communications and Interactive Systems
8.	**UCAS Code:**	
9.	**PSB Involvement:**	British Computer Society, SDS
10.	**Place of Delivery:**	GCU Glasgow City Campus
11.	**Subject Benchmark Statement:**	Computing
12.	**Dates of PSP Preparation/Revision:**	

2. EDUCATIONAL AIMS OF THE PROGRAMME

MSc Cyber Security (GA), with specialized pathway in Network Security is an applied computing programme which aims to equip graduates with the distinct specialist knowledge and analytical skills to pursue careers in the field of Cyber Security. Graduates will be able to resolve digital, cyber and network security problems, design, develop and manage computing and network solutions for the resolution of cyber security issues, have the ability to evaluate current and emergent technologies within their legal, social, ethical and industrial context. The programme will encourage apprentices' critical thinking, , expand knowledge, confidence and professional values to produce highly skilled and professional graduates able to pursue a range of careers in cybercrime investigations, digital and network security. Apprentices on this programme will combine academic study with employer specific knowledge acquisition and skills development enabling participants to become more effective and productive in the workplace.

The programme provides a stimulating broad-based education through an integrated study of vocational and academic disciplines, providing students with an enjoyable and rewarding experience that places emphasis on active and participative learning. It is based on an industrial and business-related curriculum in the theory and practice of computer science and engineering with special emphasis in the area of security governance, risk, digital forensics, ethical hacking and network security. Specifically, this programme of study provides apprentices work-based learning opportunities at a postgraduate level.

The multidisciplinary programme aims to provide apprentices with cognitive and practical skills and knowledge of new and emerging theories, methods and principles together with the practical ability to apply appropriate tools and techniques systematically. Apprentices on this programme will combine

academic study with employer specific knowledge acquisition and skills development enabling participants to become more effective and productive in the workplace.

The programme development team has worked closely with top graduate employers to ensure the learning outcomes of this programme meet the competencies required by the ICT industry. The programme has also been structured and designed to meet the core principles, skills and learning outcomes of the Skills Development Scotland Graduate Apprenticeships Framework Document for Cyber Security at SCQF level 11 [1] and is therefore designed to accommodate apprentices currently working in industry.

The programme forms part of the School and the University's commitment to provide programmes that meet the demands for current and developing technologies in society, business and industry. The aim is to integrate the expertise of staff gained from research, consultancy and scholarly activity into the programme delivery as appropriate. The school has a strong ethos of providing career-oriented learning experiences and has established itself as an approved provider for professional certifications, notably from Cisco, Microsoft, VMWare, Palo Alto, Linux and Oracle. We aim to sustain existing and seek further industrial partnerships that provide access to case studies and projects, work experience and real-world problems. The programme has been developed to address contemporary issues in the developing field of cyber security. The School will work closely with the Glasgow School for Business and Society (GSBS) in providing an inter-disciplinary approach, to teach risk management and the legal framework surrounding the use of computers, particularly with regard to privacy, freedom of information and powers of investigation.

The programme equips graduates with the transferable skills required for future academic, professional and personal development. The programme addresses the rapidly emerging need for skilled professionals in the developing specialist areas of governance, risk, digital forensics, ethical hacking and malware analysis. We would expect apprentices from a range of career pathways including government agencies, law enforcement or industry practitioners, supporting specialist roles such as forensic practitioners, penetration testers (ethical hackers),cyber security and network security consultants. The multidisciplinary nature of the programme provides a range of subjects to facilitate the development of abilities, pursuit of interests and promotion of wider career opportunities and choices.

The broad educational aims of the programme are to provide graduates with:

- a stimulating curriculum which combines study of core technological concepts, theories and principles in addition to specialised knowledge, analytical and problem solving skills in the area of cyber security. The programme of study will enable graduates to make a significant contribution to industry and society as professional practitioners;
- an understanding of scientific and engineering systems approaches encompassing the themes of digital security, digital forensics, governance, network security technologies and systems, programming for networks, communication networks and the practicalities of information and security systems, including compliance with appropriate standards in order to cope adequately with current and emerging technologies;
- skills to identify, analyse, specify, design, test and implement information systems and security of an organisation to support achievement of its business goals, and to specify and develop elements of a secure digital system, integrating hardware, software and business elements;
- a range of problem solving strategies to enable the application of knowledge in a flexible manner;
- the ability to think clearly, rationally, logically, and draw independent conclusions based on rigorous, analytical and critical assessment of arguments, opinions and data;
- skills in the use of digital technologies and relevant aspects of information technology;
- an understanding of the legal and ethical issues and concepts relating to digital systems and security, together with the audit procedures for assessing security systems and controls;

[1] https://www.skillsdevelopmentscotland.co.uk/media/43865/cyber-security-11.pdf

- an appreciation of the social impact of digital security and digital forensics, together with the ability to act in a professional and ethical manner in the development and use of digital systems, in general, and in the analysis, documentation and presentation of digital forensics cases in particular.
- the skills that enables effective communication (in writing and orally) at the appropriate business and technical level with users, management, customers and technical specialists in such a way as to meet legal regulations, requirements and audit trails and be able to present digital evidence in court;
- an extension of analytical, creative and intellectual skills to enhance and improve judgement in decision making;
- the opportunities to develop interpersonal and key soft skills, through significant exposure to team-based projects and problem-based learning;
- a sound understanding and awareness of commercial, social and business factors which influence technical solutions to solve problems.
- a range of general transferable and marketable skills, knowledge relevant to employment in a variety of roles both within the field and associated industries, together with the personal attitudes and determination necessary for professional development and further study to enable the student to make a valuable contribution throughout a successful career.

2.1 Programme Philosophy

The philosophy of this programme is to produce multi-disciplinary professional Graduate Apprentices (GA) with a bias towards cyber security. The programme aims to produce apprentices who have the required knowledge and understanding of specific digital security principles integrated with an understanding of governance, risk assessment & management, forensics, security testing, intrusion detection and security architecture reinforced with good personal, inter-personal, team working and project management skills, to enable them to perform effectively in any appropriate work environment. This is reinforced through significant formal integration of Work Based Learning opportunities and Academic Assessment as negotiated with employers.

The programme adopts the philosophy of providing an educational programme that incorporates the professional requirements throughout the curriculum. The programme has been designed to satisfy the requirements for professional membership of the BCS (The Chartered Institute for IT) accreditation, Chartered IT Professional in complex and unpredictable situations. Chartered IT Professional (CITP) status after gaining the necessary professional experience. There is an expectation apprentices will exercise leadership, initiative, personal responsibility and decision making.

The delivery of our Graduate Apprentice programmes differs from our existing postgraduate full and part-time delivery models. We recognise the approach based on work-based principles requires careful execution to exploit the work-based pedagogy and the significant benefits that are afforded through effective work-based learning as described in the Skills Development Scotland Work-based Principles[2] document and the SDS GA / SCQF Level 11 Framework.

Application of the programme philosophy will produce professionals who are able to combine established scientific and engineering professional good practice and technical skills with the ability to work effectively in the field of digital security, solving cyber related problems, providing systems to address digital security issues, address issues associated with computer crime and enhance the quality of society by making computer systems more secure and robust.

2.2 Expected Levels of Attainment

On successful completion of the programme an apprentice will be able to:

- critically evaluate problem situations within cyber security, digital security and network security contexts.
- determine appropriate approaches to cyber, digital and network security solutions.

[2] https://www.skillsdevelopmentscotland.co.uk/media/42493/gla_wbl_principles.pdf

- be able to use advanced knowledge and techniques in the construction of digital and network security solutions.
- apply the knowledge and skills from the programme directly in a work based context.

4. PROGRAMME STRUCTURES AND REQUIREMENTS, LEVELS, MODULES, CREDITS AND AWARDS

Students will undertake three modules totalling 45 credits in trimester A and trimester B. Two modules totalling 30 credits run 'long-thin' in both trimester A and B, with assessment in trimester B. The MSc Project modue (60 credits) runs in trimester C. All modules on the programme are SCQF Level 11 modules. The module descriptors contain a substantial element of Work Based Learning, which is defined as the reflection upon the theoretical learning for each module within the work place and the application of newly learned concepts to the work environment. Where appropriate, work Based Assessment is used as identified in the individual module descriptors. Appendix 4 highlights both Work Based Learning and Work Based Assessment for individual modules as a percentage.

Apprentices will not be in Full-Time on-campus attendance mode and each Trimester will have a GA specific timetable, with a combination of traditional module delivery and 'flipped classroom' sessions as appropriate.

Trimester	Module Code	Module Title	Credit
A	MMI125233	Layer 2 Technologies and Protocol Independent Routing	15
	MMI125236	Secure Operations	15
	MMI125226	Cyber Defence and Penetration Testing	15
	MMI125235	Research and Project Methods (A+B)	-
	MMI125227	Information Security Management (A+B)	-
B	MMI125225	Cyber Forensics and Incident Response	15
	MMI125237	VPN and Security Technologies	15
	MMI125234	Network Security	15
	MMI125235	Research and Project Methods (A+B)	15
	MMI125227	Information Security Management (A+B)	15
C	MMI125238	MSc Project	60
Exit awards			
PgC. Cyber Security (Requires 60 credit points) ***PgD. Cyber Security (Requires 120 credit points)*** ***MSc. Cyber Security (Requires 180 credit points)***			

8. ASSESSMENT REGULATIONS

Students should expect to complete their programme of study under the Regulations that were in place at the commencement of their studies on that programme, unless proposed changes to University Regulations are advantageous to students.

The Glasgow Caledonian University Assessment Regulations which apply to this programme, dependent on year of entry and with the following approved exceptions can be found at:

GCU Assessment Regulations

An overview of assessment details are provided in the Student Handbook for the programme and a copy of full assessment regulations are available from the University web site. Minimum pass mark is 50%, with no assessment element under 45% for all taught modules. The MSc Project has a pass mark of 50%.

The MSc Cyber Security (GA) programme is part of the Postgraduate Networking Programme Suite and subject to a specific regulation stating that a student must pass the Research and Project Methods module prior to progressing to the Dissertation (Case 52 – a minor approved exception to regulation 15.5 of the assessment regulations). The purpose of this exception is to ensure that students will have a satisfactory project proposal, which leads into the dissertation. The exception will continue to be utilised by all programmes in the suite.

• The award of the Postgraduate Certificate in Cyber Security shall be made to students who are ineligible for a higher level of award and have achieved a minimum of 60 credits with a minimum of 40 at SHEM level. (excluding the project module)

• The award of the Postgraduate Diploma in Cyber Security shall be made to students who achieve at least 120 credits with a minimum of 90 being at the SHEM level. (excluding the project module)

• The award of the Postgraduate Diploma with Distinction in Cyber Security shall normally be granted to a candidate who is eligible for the Postgraduate Diploma and has achieved an overall average of 70% or more and no mark below 55% in any module. (excluding the project module)

• The award of Master of Science in Cyber Security shall be made to students who have achieved at least 180 credits with a minimum of 150 at SHEM level. Students must pass the Research and Project Methods Module before progressing to the MSc Project (Ref)

• The award of the Master of Science with Distinction in Cyber Security shall normally be granted to a candidate who is eligible for the award of Master of Science and achieved an overall average of 70% or more with no mark below 55% in any module, and have gained at least 70% in the project module.

Role of External Examiner

External Assessors are appointed to Postgraduate Assessment Boards. The duties of an External Assessor will include the following:

- To moderate the work of the Internal Assessors in respect of the assessments under his/her jurisdiction
- To attend Assessment Boards at which the results of a final stage assessment will be determined
- To satisfy himself/herself that the work and decisions of the Assessment Board(s) are consistent with the policies and regulations of the University and best practice in higher education
- To ensure that students are assessed within the regulations approved by the University for the programme and to inform the University on any matter which, in his/her view, militates against the maintenance of proper academic standards
- To report annually to the School's Learning and Teaching Committee on the standards attained by students on the programme and on any other matters which may seem appropriate for report