GLASGOW CALEDONIAN UNIVERSITY

Programme Specification Pro-forma (PSP)

1. GENERAL INFORMATION

1.	**Programme Title:**	MSc Cyber Security (GA) MSc Cyber Security
2.	**Final Award:**	MSc Cyber Security
3.	**Exit Awards:**	PgC / PgD Cyber Security
4.	**Awarding Body:**	Glasgow Caledonian University
5.	**Period of Approval:**	From September 2020 to 2024
6.	**School:**	School of Computing, Engineering and Built Environment
7.	**Host Department:**	Department of Cyber Security and Networks
8.	**UCAS Code:**	n/a
9.	**PSB Involvement:**	Skills Development Scotland
10.	**Place of Delivery:**	GCU Glasgow City Campus
11.	**Subject Benchmark Statement:**	Computing
12.	**Dates of PSP Preparation/Revision:**	14 November 2019

2. EDUCATIONAL AIMS OF THE PROGRAMME

MSc Cyber Security (GA and full-time) 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 should 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 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;
- 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 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.

2.2 Expected Levels of Attainment

On successful completion of the programme an student should 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.
- be able to use advanced knowledge and techniques in the construction of digital and network security solutions.
- be able to apply the knowledge and skills from the programme in a work based context.

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

Section 4A – Graduate Apprenticeship mode

Graduate Apprentices will undertake two modules trimesters A, B and C of year 1. In year 2 they will take 2 modules in trimester A and work on their MSc project in trimesters B and C. All modules on the programme are SCQF Level 11 modules. Where appropriate, work based learning and assessment is used as identified in the individual module descriptors.

Trimester	Module Code	Module Title	Credit
Year 1	MMI125978	Fundamentals of routing and Switching	15
Tri A	MMI125236	Secure Operations	15
Tri B	MMI125225	Cyber Forensics and Incident Response	15
	MMI125234	Network Security	15
Tri C	MMI125235	Research and Project Methods	15
	MMI125227	Information Security Management	15
Year 2	MMI125979	Secure Connectivity	15
Tri A	MMI125226	Cyber Defence and Penetration Testing	15
Tri B	MMI125238	MSc Project	-
Tri C	MMI125238	MSc Project	60
Exit awards			
PgC. Cyber Security (Requires 60 credit points from modules listed above) ***PgD. Cyber Security (Requires 120 credit points from modules listed above)*** ***MSc. Cyber Security (Requires 180 credit points from modules listed above)***			

Section 4B – Full-time mode

Full-time students will undertake the Research and Project Methods in trimesters A and B (long-thin) to give students time to assimilate and apply the information before proceeding to the MSc stage. The MSc Project module (60 credits) runs in trimester C. All modules on the programme are SCQF Level 11 modules.

Trimester	Module Code	Module Title	Credit
A	MMI126275	Fundamentals of Routing and Switching	15
	MMI126277	Secure Operations	15
	MMI126271	Cyber Defence and Penetration Testing	15
	MMI123178	Research and Project Methods (A+B)	-
B	MMI126272	Cyber Forensics and Incident Response	15
	MMI126276	Secure Connectivity	15
	MMI126274	Network Security	15
	MMI123178	Research and Project Methods (A+B)	15
	MMI126273	Information Security Management	15
C	MMI123177	Masters Project	60
Exit awards			
PgC. Cyber Security (Requires 60 credit points from modules listed above) ***PgD. Cyber Security (Requires 120 credit points from modules listed above)*** ***MSc. Cyber Security (Requires 180 credit points from modules listed above)***			

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 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.