GLASGOW CALEDONIAN UNIVERSITY

Programme Specification Pro-forma (PSP)

1. GENERAL INFORMATION

1.	**Programme Title:**	Graduate Apprenticeship in BSc/BSc (Hons) Cyber Security
2.	**Final Award:**	BSc (Hons)
3.	**Exit Awards:**	Bachelor of Science (unclassified) Cyber Security Diploma of Higher Education in Cyber Security Certificate of Higher Education in Cyber Security
4.	**Awarding Body:**	Glasgow Caledonian University
5.	**Period of Approval:**	2021-2026
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:**	British Computer Society (BCS), Skills Development Scotland (SDS)
10.	**Place of Delivery:**	GCU Glasgow City Campus
11.	**Subject Benchmark Statement:**	EC^{UK} UK-SPEC; Computing Benchmark Statement
12.	**Dates of PSP Preparation/Revision:**	June 2021

2. EDUCATIONAL AIMS OF THE PROGRAMME

The Graduate Apprenticeship BSc/BSc (Hons) Cyber Security programme is an applied computing programme which aims to produce graduates with the distinct specialist knowledge and skills required to resolve digital security problems, design, develop and manage computing and network solutions for the resolution of cyber security activities, be knowledgeable of current and emergent technologies, understand legal, social, ethical and professional responsibilities of practitioners and have a broad awareness of industry. The programme will encourage apprentices' creative thinking, expansion of knowledge, confidence and professional values so producing highly skilled and professional graduates able to pursue a range of careers in cybercrime investigations and digital 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 areas of security governance, risk, digital forensics and ethical hacking. Specifically, this programme of study provides apprentices with work-based learning opportunities at a BSc/BSc (Hons) 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 10[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, guru lectures 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 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 associated private sector agencies, supporting specialist roles such as forensic practitioners, penetration testers (ethical hackers) and cyber security consultants as well as organisations that recruit IT specific graduates such as supermarkets, banks etc. that have job roles for graduates with a cyber security background. The multidisciplinary nature of the programme

[1] https://www.skillsdevelopmentscotland.co.uk/media/43673/cyber-security-framework-l10.pdf

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 and understanding 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;
- a range of analytical and modelling methods for use in scientific and engineering applications within the digital security specialism to specify and design secure digital networks and systems;
- 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 awareness 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 enable 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 at each level of the programme.

The programme adopts the philosophy of providing an educational programme that incorporates the professional requirements throughout the module syllabus. The BEng exit pathways correspond with the graduate as technical specialist (supporting the need for technology “innovators”) with technical expertise enhanced in selected niche areas. The programme has been designed to satisfy the requirements for professional membership of the BCS (The Chartered Institute for IT) accreditation to contribute to the expectations to provide partial fulfilment of the competence and commitment required to prepare graduates to progress to Chartered Engineer (CEng), Chartered IT Professional (CTIP) 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 undergraduate 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 affords through effective work-based learning as described in the Skills Development Scotland Work-based Principles[2] document and the SDS GLA Cyber Security Level 10 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 level 1 an apprentice should have a basic knowledge of the software and hardware concepts which underpin modern computing systems.
- On successful completion of level 2 an apprentice should have a sound knowledge of digital security principles and concepts and show competence in applying this to a range of digital security domains.
- On successful completion of level 3 an apprentice should be able to plan, specify, design, implement and support components of a digital security system in response to a business need in accordance with fundamental principles and methods, using appropriate techniques and tools.
- On successful completion of level H an apprentice will, in addition, be able to critically evaluate alternative approaches to digital security solutions and be able to use advanced knowledge and techniques in the construction of a digital security solution.

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

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

There will be a minimum of 40 credits per trimester. Level 1 & 2 will have a minimum of 20 credits of Work Based Assessment over the academic year. Level 3 & 4 will have a minimum of 40 credits of Work Based Assessment over the academic year. Trimester C has a lighter taught module load throughout the programme since it includes the project modules which are work based. There will also be the possibility of negotiated Work Based Assessment for a number of other modules if possible as identified in the individual module descriptors. The module descriptors also contain an allocation to 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. Appendix 4 highlights both Work Based Learning and Work Based Assessment for individual modules as a percentage.

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

Year	Module Code	Module Title	Credit	Trimester
1 (SCQF7)	M1I326581	Programming for Cyber Security & Networks 1[1,3]	20	A
	M1I325085	Mathematics for Computing[1,3]	20	AB
	M1I325893	Fundamentals of Computing Systems[1]	10	A
	M1I125225	Computer Networking 1[1,3]	20	B
	M1I325898	Cyber Security Landscape[1,3]	10	B
	M1I325894	Database Development[1]	20	C
	M1I126859	Cloud Foundations and Machine Learning[1]	20	C
Certificate of Higher Education in Cyber Security				
2 (SCQF8)	M2G426861	Ethical Hacking[1]	20	A
	M2G425229	Computer Networking 2[1,3]	20	A
	M2I326554	Web Application Development 1[1,3]	20	B
	M2G426860	Digital Forensics 1[1,3]	20	B
	M2G426865	Programming for Cyber Security & Networks 2[1,3]	20	C
	M2H625231	Integrated Design Project 2[2]	20	C
Diploma of Higher Education in Cyber Security				
3 (SCQF9)	M3I126867	Digital Forensics 2[1,3]	20	A
	M3I126866	Malware Analysis and Exploits 1[1,3]	20	A
	M3G426870	Security Operations Analysis[1,3]	20	B
	M3G426862	Applied Penetration Testing[1]	20	B
	M3H626863	Cloud Operations[1,3]	20	C
	M3I325099	Research Skills and Professional Issues[1,2]	20	C
Batchelor of Science (unclassified) Cyber Security				
4 (SCQF10)	MHH126864	Cyber Physical Systems Security[1,3]	20	A
	MHH126583	Artificial Intelligence for Cyber Security[1,3]	20	A
	MHI125244	Web Application Security[1,3]	20	B
	MHI226868	Malware Analysis and Exploits 2[1,3]	20	B
	MHW226542	Honours Project[2,3,4]	40	ABC
Batchelor of Science (Hons) Cyber Security				

Notes

1. Modules are delivered via a ‘Flipped Classroom’ mode with dedicated seminar sessions in the timetable requiring attendance at GCU.
2. Work-based modules that require minimal contact. Any class contact required and the detail of the module will be captured in the apprentices Individual Learning and Training Assessment Plan.
3. Modules that can have negotiated or generic work-based learning & assessment contextualised to the individual’s work environment.
4. The final year project will be completed over 12 full-time weeks in the work place. At 35 hours / week, this would be 420 hours which is greater than the notional contribution for a 40 credit module of 400 hours.

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 can be found at:

GCU Assessment Regulations

Role of External Examiner

External Assessors are appointed to Undergraduate 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