GLASGOW CALEDONIAN UNIVERSITY

Programme Specification Pro-forma (PSP)

1.	GENERAL INFORMATION	
1.	**Programme Title:**	Graduate Apprenticeship in BSc (Hons) Cyber Security
2.	**Final Award:**	Graduate Apprenticeship in Bachelor of Science with Honours in Cyber Security
3.	**Exit Awards:**	Graduate Apprenticeship in Bachelor of Science 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 rovides 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.

3. INTENDED LEARNING OUTCOMES

The development of this programme has been informed by:

- GCU Qualifications framework, GCUQF – v6 2015
- QAA Subject Benchmark Statement Computing 2016
- "The Accreditation of Higher Education Programmes" Engineering Council UK Standard for Professional Engineering Competences (UK-SPEC) August 2020
- BCS Guidelines on Course Accreditation, Jan 2020.
- The requirements documented in the Skills Development Scotland Graduate Apprenticeships Framework document for Cyber Security at SCQF Level 10 Framework (Appendix 2: BSC / BSc(Hons) Cyber Security (GA) / Framework for Cyber Security at SCQF Level 10 Mapping).

3A Knowledge and understanding;

A1: Demonstrate an understanding of the scientific and mathematical principles underpinning the programme of study and the ability to apply mathematical methods, tools and notations proficiently in the analysis and solution to problems.

A2: Demonstrate knowledge and understanding of the essential facts, concepts and theories relating to technological applications as appropriate to cyber security, together with an awareness of the development of digital technologies.

A3: Demonstrate the use of such knowledge and understanding in the modelling and design of computer-based systems for the purposes of comprehension, communication, prediction and the understanding and trade-offs.

A4: Demonstrate the use of scientific principles in the creation, use and support of systems for the solution of practical problems within cyber security.

A5: Demonstrate the ability to analyse the extent to which a computer-based system meets the criteria defined for its current use and future development.

A6: Demonstrate knowledge and understanding of the commercial and economic context of the design, development, use and maintenance of digital systems.

A7: Demonstrate knowledge and understanding of the management techniques used to achieve objectives within a computing context.

A8: Demonstrate an understanding of the legal system and the framework of relevant legal processes, regulatory environments, codes of practice, quality issues and industrial standards, involved in the exploitation of digital technology.

A9: Understand the multi-disciplinary nature of the subject area, the need for a high level of professional and ethical conduct in practice, and, the requirement for cyber activities to promote sustainable development.

3B Practice: Applied knowledge, skills and understanding;

B1: Demonstrate the ability to specify design and construct computer based systems.

B2: Demonstrate the ability to evaluate systems in terms of general quality attributes and possible trade-offs presented within the given cyber related problem.

B3: Demonstrate the ability to recognise any risks or safety aspects that may be involved in the operation of computing and information systems within a given cyber context.

B4: Demonstrate the ability to deploy effectively the tools used for the construction and documentation of computer applications with particular emphasis on understanding the whole process involved in the effective deployment of computers to solve practical problems.

B5: Demonstrate the use of appropriate and practical processes to specify and design, implement, verify and maintain computer based systems including working with technical uncertainty.

B6: Define a problem, research its background, understand the social and cultural context, identify constraints, understand consumer and user needs, identify and manage cost drivers, ensure fitness for purpose and manage the design process and evaluate outcomes.

3C Generic cognitive skills:

C1: Demonstrate logical thinking and problem solving.

C2: Critical analysis / evaluate work undertaken by themselves and others.

C3: Demonstrate effective information management, retrieval and research skills for independent enquiry and learning.

C4: Evaluate alternative solutions to problems in an appropriate subject domain.

3D Communication, numeracy and ICT skills:

D1: Demonstrate communication skills (Electronic, written, oral and listening) necessary to make effective presentation of a technical nature (information, ideas, problems and their solution) to a

range of audiences.

D2: Demonstrate numeracy in both understanding and presenting cases involving a quantitative dimension.

3E Autonomy, accountability and working with others:

E1: Demonstrate an awareness of my strengths and weaknesses E2: Demonstrate creativity, innovation and independent thinking.

E3: Demonstrate an appreciation and desire for the need to reflect, and plan for self-learning and improving performance as the foundation for CPD and life-long learning.

E4: Demonstrate reliability, integrity, honesty and ethical awareness. E6: Demonstrate entrepreneurial, independence and risk taking.

E6: Demonstrate the ability to prioritise tasks and time management (organising and planning work).

E7: Demonstrate effective interpersonal skills, the ability to work as a member of a team (work with and relate effectively to others) recognising the different roles within a team and different ways of organising teams (leadership).

Students in related employment which provides the opportunity for further development of the taught practical, personal and professional skills in a work-based environment.

F1 Gain additional competence and training in the application of the practical skills within cyber security.

F2 Develop an understanding of the practical considerations that constrain the application of theory in the workplace.

F3 Communicate and interact effectively within a work-based situation

F4 Evaluate current research and technology concepts and their relationship and application to a work- based problem within a cyber context

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

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
Graduate Apprenticeship in Bachelor of Science 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
Graduate Apprenticeship in Bachelor of Science with Honours in 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.

6. CRITERIA FOR ADMISSION

Candidates must be able to satisfy the general admissions requirements of Glasgow Caledonian University

Candidates for the programme will normally be at least 16 years of age at the start of the programme, be in suitable employment as an apprentice and meet the following entry requirements.

Programme Admission Requirements:

Standard First Year Entry Requirements

The minimum entrance requirements for entry into the first year of the programme are one of the following:

- SQA passes in 5 subjects of which at least 4 are at Higher Grades at BBBB or above, or 3 A Level Grades at CCC or equivalent. Essential subject is Mathematics (Higher)
- GCE passes in 5 subjects of which 2 are Advanced level (or equivalent)
- An appropriate program of SQA National Certificate Course units which must include passes in modules which are at least equivalent to SQA/GCE English and Mathematics at Ordinary/ Standard grade at Credit level
- HNC in Computing/IT or Equivalent
- BTEC National Diploma in Computing/IT
- Irish Leaving Certificate – 5 subjects passed at H level (at least C grade) or equivalent
- International qualifications which are equivalent to standard entry (in these cases appropriate EOSL qualification is required)

In all of the above cases, the qualifications must include SCE/GCE pass in English at Standard grade at Credit level (or equivalent) and Mathematics at Higher Grade C (or equivalent)

Annually the Programme Board also considers the competitive entry requirements based on apprentice demand and allocated places.

Flexible Entry - Credit Transfer and Recognition of Prior Learning (RPL):

Integration of flexible entry and RPL are integral to the delivery within this programme.
Accumulation of credit points from other programmes of study and from prior experiential learning may allow direct entry into the programme at the appropriate level, subject to satisfying the necessary pre- requisites for completion of the programme.

Entry with Advanced Standing:

Articulation to Level 2 and Level 3

Companies are encouraged to put forward apprentices for possible entry to L2 and L3 through the GCU accreditation of prior learning route. This is applicable to current employees with many years

of experience and some formal qualifications or to new apprentices who have achieved qualifications from further education study.

Mature
Formal entry requirements may be relaxed for mature applicants (21 years of age and older) whose record of educational achievement and relevant experience is deemed to be appropriate.

Equal Opportunities
The University will seek at all times equality of opportunity for all applicants and seeks not to discriminate on any grounds irrelevant to the above general principle of admission.

Applicants with a Disability
All applicants for admission to the programme who reveal a disability will be invited to a meeting with the Admissions Tutor and/or University Disability Adviser in order that the specific needs of the applicant can be assessed. This is not part of the selection process but students may be advised at this stage if the nature of their disability means that they might be unable to fulfil the academic or professional requirements of the programme. Equally it may not be possible for the University to make reasonable adaptations to enable an applicant to undertake a particular programme. Should this be the case, the University will respond positively and advice on alternative programmes and options will be offered

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