GLASGOW CALEDONIAN UNIVERSITY

Programme Specification Pro-forma (PSP)

1.	**GENERAL INFORMATION**	
1.	**Programme Title:**	BSc(Hons) Cyber Security & Networks
2.	**Final Award:**	BSc(Hons) Cyber Security & Networks BSc(Hons) Cyber Security & Networks (Sandwich)
3.	**Exit Awards:**	BSc Cyber Security & Networks Diploma of Higher Education in Cyber Security and Networks Certificate of Higher Education in Cyber Security and Networks
4.	**Awarding Body:**	Glasgow Caledonian University
5.	**Period of Approval:**	2021-2026
6.	**School:**	School of Computing, Engineering and Built Environment.
7.	**Host Department:**	Cyber Security & Networks
8.	**UCAS Code:**	
9.	**PSB Involvement:**	The Chartered Institute for IT (BCS)
10.	**Place of Delivery:**	GCU
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 philosophy of the BSc/BSc (Honours) Cyber Security and Networks programme is to provide 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 a broader industrial and business-related curriculum that combines a subset of technical skills with expertise in selected other discipline areas.
The programme aims to provide graduates with cognitive and practical skills and knowledge of emerging theories, methods and principles. The aim is to establish well-rounded graduates knowledgeable of current and emergent technologies, understand legal, ethical and professional responsibilities of practitioners and have a broad awareness of industry. The programme will encourage students' creative thinking, develop visualization skills, expand knowledge, confidence and professional values.

The programme is taught within a wider suite of programmes related to the disciplines of Cyber Security and Networking. Sharing a common first two years within the suite, the programme provides an opportunity to explore specialisms within the general theme of Computer Networking and Digital Security, together with those that are core to the understanding of scientific and engineering disciplines, and technological principles. This provides students with experience of, and the

opportunity to transfer to the other programme within the suite, assuming existing admission requirements are met.

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, Red Hat, Palo Alto, LogRythm. 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 new programme has been developed to address contemporary issues in the field of cybersecurity and networking.

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 information systems and network infrastructures. The programme equips graduates with the transferable skills required for future academic and personal development.

2.2 General Aims of the Programme

The programme aims to provide graduates with cognitive, practical, self-management skills and knowledge of theoretical, professional, technical, legal and social aspects to be able to pursue careers in Cybersecurity and Networking. It aims 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 and network infrastructure technologies enabling 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 network engineering, programming for networks, security systems theory, communications networks and the practicalities of network 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 to specify and design secure digital networks and systems;
- Skills to specify, design 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 networked system, integrating hardware, software and business elements;
- A range of problem solving strategies to enable the application of knowledge;
- The ability to think clearly, rationally, logically, and draw independent conclusions based on 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 engineering, including ethical and environmental consequences and considerations.
- The skills that enables effective communication (in writing and orally) at the appropriate business and technical level with users, management, customers and technical specialists;
- 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.

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

SCQF Level 7 – Year 1

Module Code	Module Title	Credit
M1I124450	Computer Networking 1	20
M1I326580	Programming for Cyber Security 1	20
M1I325623	Fundamentals of Computer Systems	10
M1I325851	Mathematics for Computing	20
M1I325625	Database Development	20
M1I126838	Cloud Foundations and Machine Learning	20
M1I125808	Cyber Security Landscape	10
Exit Award – Certificate of Higher Education in Cyber Security and Networks		**120**

SCQF Level 8 – Year 2

Module Code	Module Title	Credit
M2G425834	Secure Systems Administration	20
M2G424453	Computer Networking 2	20
M2G426840	Digital Forensics 1	20
M2G426839	Programming for Cybersecurity and Networks 2	20
M2G426843	Ethical Hacking	20
M2I325626	Web Application Development 1	20
Exit Award – Diploma of Higher Education in Cyber Security and Networks		**240**

SCQF Level 9 – Year 3

Module Code	Module Title	Credit
M3I126844	Internet Security	20
M3G426850	Applied Penetration Testing	20
M3H626848	Cloud Operations	20
M3G426849	Security Operation Analysis	20
M3H626847	Advanced Campus Networking	20
M3I323074	Research Skills and Professional Issues	20
Exit Award – Bachelor of Science in Cyber Security and Networks		**360**

SCQF Level 10 – Year 4

Module Code	Module Title	Credit
MHH126851	Cyber Physical Systems Security	20
MHI126852	Enterprise Networking 1	20
MHI126853	Enterprise Networking 2	20
MHI124570	Web Application Security	20
MHW225671	Honours Project	40
Exit Award – Bachelor of Science with Honours in Cyber Security and Networks		**480**

	Notes:
1.	***Student Exchange (Optional).*** After successful completion of Level 3 Trimester 1 students may be eligible to undertake an optional study exchange during Trimester 2 at an appropriate host Institution out-with the UK, provided the agreed programme of activity is equivalent to the curriculum and intended student experience undertaken in Level 3 Trimester 2. Successful completion of the study exchange is credit bearing to 40 credits and students must undertake this alongside the pre-requisite module, Research Skills & Professional Issues (CSN) (20 credits) for a total of 60 credits.
2.	***Industrial Placement Year (Optional).*** Students opting to undertake placement do so in the academic session after successfully completing their Level 3 studies and before undertaking their Honours year. Assessment is via the additional 60 SCQF level 9 module, M3I323077 Industrial Placement (CCIS). Successful completion of that module gives (Sandwich) in the final exit award obtained by the student. **Exception to Undergraduate Assessment Regulations, Sub-sections 19.4; 19.7.1; 19.8.2 Classification of Honours Award**: *that the Level 3 Industrial Placement module is excluded from the Honours Classification Calculation Set.*

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.

Exception to Undergraduate Assessment Regulations, Sub-sections 19.4; 19.7.1; 19.8.2 Classification of Honours Award: *that the Level 3 Industrial Placement module is excluded from the Honours Classification Calculation Set.*

The Glasgow Caledonian University Assessment Regulations which apply to this programme, dependent on year of entry can be found at: GCU Assessment Regulations