Modular Provision Specification

Pathway Summary Information		
1	**Pathway Title and Credits**	CyberShield: Cyber Security and Ethical Hacking (40 Credits)
2	**Course Code**	CP1030-01
3	**Awarding Institution**	Birmingham City University
4	**Teaching Institution(s)** (if different from point 3)	
5	**Professional Statutory or Regulatory Body (PSRB) accreditation** (if applicable)	

6	**Modular Provision Description**
	CyberShield: Cyber Security and Ethical Hacking is a 40-credit modular programme designed to provide a practical introduction to the principles, technologies and techniques used to protect modern digital environments. Combining Cyber Security Fundamentals and Network Fundamentals, this 40-credit programme develops the knowledge and skills needed to understand cyber threats, assess vulnerabilities and implement security measures across networked systems. Through a mixture of theory and hands-on practical activities, you'll explore how networks operate, how attacks occur, and how organisations can defend their systems and data. Eligible for Lifelong Learning Entitlement (LLE) funding, this flexible modular offer is ideal for those looking to upskill, retrain, or take their first steps into the rapidly growing cyber security sector. Content is aligned with industry-recognised practices and introduces concepts that support progression towards professional certifications and further study. Cyber security remains one of the fastest-growing areas of the digital economy, with organisations across all sectors seeking professionals who can help protect systems, data and infrastructure. These modules will allow you to develop a range of technical and professional skills valued by employers, including: • Cyber threat identification and analysis. • Risk assessment and security awareness. • Network design and configuration. • Security monitoring and mitigation techniques. • Problem-solving and technical troubleshooting. • Application of industry-standard cyber security and networking tools. • Independent learning and professional development. The combination of cyber security and networking knowledge provides a strong foundation for entry-level roles and future professional development within information technology, networking and cyber security disciplines.

7	**Module Titles and Credits Awarded:** ***In order to complete this provision a student must successfully complete the following CORE modules (totalling 40 credits):***	
	Cyber Security Fundamentals	20 credits
	Network Fundamentals	20 credits

8	**Variation from the University Regulations**
	This course has approved variations to the University's Academic Regulations. These can be accessed via the student contract page: https://www.bcu.ac.uk/student-info/student-contract

9	**Delivery Patterns**		
Mode(s) of Study	**Location(s) of Study**	**Duration of Study**	**Code(s)**
Part time	Steamhouse, City Centre	4 months	CP1030-01

10	**Entry Requirements**	
	Home:	Our typical academic entry requirement is 48 UCAS tariff points or above. However, we recognise that applicants may have gained skills and knowledge through a range of routes and will also consider applications from those who do not meet this requirement but can demonstrate achievement at Level 2 and/or Level 3, together with relevant experience. If you are returning to study and have previously completed a degree or other higher education qualification, we will accept a qualification in any discipline.

11	**Learning, Teaching and Assessment Strategy**
	Teaching takes place via lectures, practical laboratory sessions, guided activities and independent study to help you develop both theoretical understanding and technical skills. You'll investigate cyber security threats, vulnerabilities and protection mechanisms while developing practical networking competencies. Laboratory activities provide opportunities to work with networking devices, simulation software and cyber security tools used within industry. You'll learn through practical investigation, problem-solving exercises and real-world scenarios that mirror challenges faced by organisations today. The course places particular emphasis on applied learning, enabling you to develop confidence in identifying risks, implementing protection measures and understanding how secure network infrastructures are designed and managed.

Module Specification

Module Summary Information

1	**Module Title**	Cyber Security Fundamentals
2	**Module Credits**	20
3	**Module Level**	4
4	**Module Code**	CMP4298
5	**Semester Taught**	2

6	**Module Overview**
The module introduces the fundamental elements of cybersecurity and its body of knowledge. It aims to develop a firm grounding in the underpinning knowledge and skills required to protect organisations from cyber-attack. You will be introduced to cybersecurity principles and implications of threats, vulnerability and risks facing these organisations. You will acquire theoretical knowledge and practical skills in cybersecurity that you will build on as you progress through the course. You will learn about security protection measures and mitigation strategies to enable you to protect and respond to cyber-attacks. The module emphasises on the development of practical skills supported by a variety of learning activities, including lectures, practice labs, self-directed and online through Virtual Learning Environments (VLE). The weekly hands-on practical labs give you the opportunities to practice with industry-recognised tools and broaden your skills.	

7	**Indicative Content**
The module will introduce you to the following topics: • Starting a career in Cyber Security • Roles and responsibilities in Cyber security • Network Security concepts • Types of threats • Protecting systems and home networks • Internet safety and social media • Data Security and information Sharing • Basic IoT security • Fundamentals of Cryptography • Human aspect of cybersecurity	

8	**Module Learning Outcomes** **On successful completion of the module, you will be able to:**	
	1	Describe and assess the principles of cybersecurity as applied to a given scenario.
	2	Identify common cybersecurity threats and appraise mitigation strategies.
	3	Apply appropriate tools to determine and evaluate the security state for a given system.
	4	Develop effective security policies for a given scenario.

9	Module Assessment		
Learning Outcome Number *(from table 8)*	**Coursework**	**Exam**	**In-Person**
1 and 2	**X** (40%)		
3 and 4	**X** (60%)		

10	Breakdown Learning and Teaching Activities	
Learning Activities	**Hours**	**Details of Duration, Frequency and other comments**
BCU Standard Delivery:		
Scheduled Learning includes lectures, practical classes and workshops as specified in timetable. For blended learning modules, delivery can include: • In person • Asynchronous (guided, curated content) • Synchronous (live online)	*48*	*1 x 12hr Lecture Sessions* *3 x 12hr Practical Lab Sessions*
Directed Learning (non-curated) includes placements, work-based learning, peer group learning external visits, on-line activity, Graduate+, peer learning, as directed on VLE	*48*	*4hrs/wk* *Review weekly Moodle contents* *Participate in industry workshops and seminars when required.*
Private Study includes preparation for exams	*104*	*Read directed material around the discipline as instructed by the tutor/module team.* *Case studies, pre-reading articles and exercises*
Total Study Hours	*200*	

Module Specification

Module Summary Information

1	**Module Title**	Network Fundamentals
2	**Module Credits**	20
3	**Module Level**	4
4	**Module Code**	CMP4269
5	**Semester Taught**	2

6	**Module Overview**
In this module you will develop your understanding of communication over networks and how devices send and receive data over their connected networks. We will use two of the standard referencing models, OSI and TCP/IP, that will help break down all the steps involved in data transmission and devices' communication over networks using their layered approach. We will discuss the function of each layer in details and some of the protocols at each of these layers and how they help get data delivered from sender to receiver over the network. During the lab sessions, you will also learn how to build simple local area networks and how to perform basic networking device configurations using real networking devices. You will also use networking simulation programs to help you further practice your skills while working from home. This module covers the first part of CCNA curriculum (CCNA1: Introduction to Networks) which will also give you good chance to start working towards your CCNA certification which is highly regarded in networking-related careers.	

7	**Indicative Content**
During the module students will explore the following areas: - OSI and TCP/IP reference models - Physical layer and Data link layer protocols - Network layer protocols including IPv4 and IPv6 addressing schemes - Upper layer protocols and how they support different network applications - Configuration of networking devices to enable end-to-end connectivity across network	

8	**Module Learning Outcomes** **On successful completion of the module, students will be able to:**	
	1	Use standardised layered models in the analysis and design of structured communication networks.
	2	Design appropriate network system (using devices, addressing schemes, protocols, etc.) to a meet a given network specification.
	3	Deploy, manage and secure network devices.

9	**Module Assessment**		
Learning Outcome Number *(from table 8)*	**Coursework (100%)**	**Exam**	**In-Person**
1,2,3	**100%**		

10	Breakdown Learning and Teaching Activities		
Learning Activities		**Hours**	**Details of Duration, Frequency and other comments**
Scheduled Learning (SL) includes lectures, practical classes and workshops as specified in timetable		*48*	*2 hours weekly lectures* *2 hours weekly lab sessions* *x 12*
Directed Learning (DL) includes placements, work-based learning, peer group learning external visits, on-line activity, Graduate+, peer learning, as directed on VLE		*50*	*Directed reading of lecture slides + online chapters+ online quizzes* *Practical work*
Private Study (PS) includes preparation for exams		*102*	*General reading to broaden understanding of the theory and practice introduced in the module*.
Total Study Hours:		*200*	