Course Specification

Course Summary Information				
1	**Course Title**		BSc (Hons) Cyber Security – January Intake	
2	**Course Code**	**UCAS Code**	US1591	BSc (Hons) 1010
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	**Course Description**
	In today's digitally connected world, secure information technologies are the backbone of modern society. As cyber threats become increasingly sophisticated, the demand for skilled cybersecurity professionals has never been greater. The BSc Cyber Security course is designed to equip you with cutting-edge technical expertise, analytical proficiency, management capabilities, and practical skills to effectively tackle the cybersecurity challenges faced by modern organisations. Our strong links with industry enable us to teach the most demanding and up-to-date topics. **What's covered in the course?** Taking a practice-led approach, the course emphasises hands-on experience with industry-standard tools and technologies, ensuring that graduates are well-prepared for successful careers in cybersecurity. The industry-informed curriculum is structured to provide a strong foundation in security principles while fostering the critical thinking and problem-solving skills necessary to defend against cyber threats. The course benefits from a dynamic research-inspired environment and is supported by strong industry partnerships with leading organisations including CISCO, EC-Council, IBM, Microsoft and the Linux Professional Institute. These collaborations provide students with exposure to real-world cybersecurity challenges, access to professional networks, and opportunities to work with cutting-edge technologies, enhancing both learning and career prospects. In your first year, you will develop a strong foundation in computing and cybersecurity, covering essential subjects such as cybersecurity fundamentals, computer programming, computer systems, networking fundamentals, and mathematics for computing. During your second year, you will expand your knowledge through advanced cybersecurity subjects, including software security, applied cryptography, networking technologies, applied cyber forensics, and cybersecurity operations. Additionally, you will have the option to undertake a sandwich placement year between your second and final year, gaining valuable industry experience. In your final year, you will study subjects such as ethical hacking, applied artificial intelligence (AI) for cybersecurity, network & internet forensics and cloud computing. You will also complete an individual project, demonstrating your technical expertise and preparing you for career opportunities in the cybersecurity field. The final year students will take part in our annual

	Innovation Fest which is a unique opportunity for our students to showcase their creativity, problem-solving skills, and technical expertise. our students have pushed the boundaries of what is possible and created solutions to real-world challenges. Upon graduation you could progress into a career as a Cyber Security Analyst, Penetration Tester, Security Architect, Security Operations Centre (SOC) Analyst, Risk and Compliance Analyst and Cloud Security Engineer.

7	**Course Awards**		
7a	**Name of Final Award**	**Level**	**Credits Awarded**
	For BSc (Hons): Bachelor of Science with Honours Cyber Security Bachelor of Science with Honours Cyber Security with Professional Placement Year	 6 6	 360 480
7b	**Exit Awards and Credits Awarded**		
	Certificate of Higher Education Cyber Security Diploma of Higher Education Cyber Security Bachelor of Science Cyber Security	4 5 6	120 240 300

8	**Variations from the University Academic 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**	**Duration of Study**	**Code**
BSc (Hons) Full Time (January Intake)	City Centre	3 years	US1591
BSc (Hons) with Professional Placement Year (January Intake)	City Centre	4 years	US1591

10	**Entry Requirements**
	The admission requirements for this course are stated on the course page of the BCU website at https://www.bcu.ac.uk/.

11	**Course Learning Outcomes**
	Knowledge & Understanding
1	Demonstrate knowledge and understanding of key cyber security concepts, mechanisms, services and protocols that are used as basic building blocks for engineering security solutions.
2	Analyse trends of cyber-attacks, evolving security threats, the mechanisms for monitoring and detecting them, protection controls for mitigating their risks and approaches for holistic cyber defence.
3	Apply best practices for security management within an enterprise abiding by legal obligations, regulatory requirements, international standards, ethical considerations, good governance, incident response and business continuity plans.
4	Demonstrate knowledge and understanding of cyber security topics such as network security, digital forensics, AI, information assurance, security testing, threat modelling and secure software development.
	Cognitive & Intellectual Skills
5	Systematically analyse security threats to information assets of an organisation, propose suitable countermeasures and justify choices using relevant quantitative and qualitative methods for evaluating associated business risk.
6	Evaluate the conformance of security management processes of an organisation against international security standards, such as ISO 27000, identifying gaps and recommend mitigations
7	Apply design principles such as least privileges, fail secure, and defence in depth to engineer security, privacy and resilience.
8	Analyse and correlate digital forensic information from a variety of sources such as audit logs, hard disks, operating systems, file systems and web browsers in order to detect breaches of security policy, law or regulations.
	Practical & Professional Skills
9	Utilise digital forensic tools for collecting, analysing, and processing electronic evidence through application of forensically sound methodologies.
10	Demonstrate hands-on experience of security testing tools to systematically identify certain types of vulnerabilities in communication network infrastructures.
11	Apply appropriate tools to manage threats against software or systems.
12	Propose a contingency plan, consistent with the organisation's view of associated risks, to ensure business continuity for an organisation upon the detection of an adverse event
	Key Transferable Skills
13	Apply skills in research, independent study, career planning, self-management, including time management and prioritisation of tasks when tackling complex problems.
14	Demonstrate effective communication skills in writing, orally, and in presentations to specialist and non-specialist audiences. Be able to explain, justify and otherwise defend their work and ideas, both in its specific details and within a broader context
15	Demonstrate team-spirit by cooperating with others, plan and implement tasks at a professional level and contribute to team goals through making sound judgments.
16	Develop confidence and a resilient approach to undertake a substantial piece of practical work without close supervision.

12	Course Requirements

12a

Level 4:

In order to complete this course a student must successfully complete all the following CORE modules (totalling 120 credits):

Module Code	Module Name	Credit Value
CMP4267	Computer Systems	20
CMP4298	Cyber Security Fundamentals	20
CMP4265	Applied Operating Systems	20
CMP4266	Computer Programming	20
CMP4268	Mathematics for Computing	20
CMP4269	Network Fundamentals	20

Level 5:

In order to complete this course a student must successfully complete all the following CORE modules (totalling 120 credits):

Module Code	Module Name	Credit Value
CMP5358	Software Security	20
CMP5319	Systems Security Attacks and Defences	20
CMP5372	Applied Cyber Forensics	20
CMP5357	Cyber Security Operations	20
CMP5320	Networking Technologies	20
CMP5385	Applied Cryptography	20

Professional Placement Year (optional) - ***In order to qualify for the award of Bachelor of Science with Honours Cyber Security with Professional Placement Year, a student must successfully complete all of the modules listed as well as the following Level 5 module:***

Module Code	Module Name	Credit Value
PPY5004	Professional Placement	120

Level 6:

In order to complete this course a student must successfully complete all the following CORE modules (totalling 120 credits):

Module Code	Module Name	Credit Value
CMP6200	Individual Honours Project	40
CMP6176	Ethical Hacking	20
CMP6238	Applied AI for Cyber Security	20
CMP6189	Network and Internet Forensics	20
CMP6210	Cloud Computing	20

12b Structure Diagram

Level 4

SEMESTER ONE (January Start)	SEMESTER TWO (MAY Start)
Core CMP4266 Computer Programming CMP4267 Computer Systems CMP4268 Mathematics for Computing	**Core** CMP4298 Cyber Security Fundamentals CMP4265 Applied Operating Systems CMP4269 Network Fundamentals

Level 5

Core CMP5358 Software Security CMP5385 Applied Cryptography CMP5320 Networking Technologies	**Core** CMP5357 Cyber Security Operations CMP5319 System Security Attacks and Defenses CMP5372 Applied Cyber Forensics

Professional Placement Year 4 (optional) Professional Placement Module (120 Credits)

Level 6

Core CMP6238 Applied AI for Cyber Security CMP6189 Network and Internet Forensics	**Core** CMP6176 Ethical Hacking CMP6210 Cloud Computing
Core CMP6200 Individual Honours Project (40 Credits)	

13 Overall Student Workload and Balance of Assessment

Overall student *workload* consists of class contact hours, independent learning and assessment activity, with each credit taken equating to a total study time of around 10 hours. While actual contact hours may depend on the optional modules selected, the following information gives an indication of how much time students will need to allocate to different activities at each level of the course.

Scheduled Learning includes lectures, practical classes and workshops, contact time specified in timetable
Directed Learning includes placements, work-based learning, external visits, on-line activity, Graduate+, peer learning

Private Study includes preparation for exams

The *balance of assessment* by mode of assessment (e.g. coursework, exam and in-person) depends to some extent on the optional modules chosen by students. The approximate percentage of the course assessed by coursework, exam and in-person is shown below.

Level 4

Workload

24% time spent in timetabled teaching and learning activity

Activity	Number of Hours
Scheduled Learning	292
Directed Learning	469
Private Study	439
Total Hours	1200

Balance of Assessment

Assessment Mode	Percentage
Coursework	80%
Exam	20%
In-Person	0

Level 5

Workload

24% time spent in timetabled teaching and learning activity

Activity	Number of Hours
Scheduled Learning	288
Directed Learning	532
Private Study	380
Total Hours	1200

Balance of Assessment

Assessment Mode	Percentage
Coursework	70%
Exam	22%
In-Person	8%

Level 6

Workload

17% time spent in timetabled teaching and learning activity

Activity	Number of Hours
Scheduled Learning	202
Directed Learning	334
Private Study	664
Total Hours	1200

Balance of Assessment

Assessment Mode	Percentage
Coursework	94%
Exam	0%
In-Person	6%