Course Specification

Course Summary Information				
1	**Course Title**		BSc (Hons) / MSci Cyber Security	
2	**Course Code**	**UCAS Code**	BSc (Hons) US0937 MSci UM0044	BSc (Hons) 1010 MSci 1011
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**
	The BSc/MSci Cyber Security course is designed to equip you with state-of-the-art technical knowledge, intellectual know-how, management capabilities and practical skills that will enable you to succeed in meeting the cyber security challenges facing modern organisations. In the 21st century, data has become a necessary commodity, which has value in isolation and more so when viewed as a larger data set for trends and habits. Data is key to the functioning of modern business and the protection of this data is key to the ongoing success of the digital economy. As systems, such as IoT, both generate and consume data grow in capability and complexity, the need to protect the data created, stored and transited across public and private networks intensifies. Due to this, the need for suitably qualified cyber security practitioners has never been greater. This course will provide you with the knowledge and skills needed by the employers. Our strong links with industry enable us to teach the most demanding and up-to-date topics. You will learn state of the art technical knowledge, intellectual know-how, management capabilities and hands-on practical skills to succeed in meeting the cyber security challenges faced by modern organisations. This course is supported by a vibrant research environment within the centres for Cyber Security and Cloud Computing at BCU and by traditionally strong industrial links with CISCO, Oracle, IBM, Microsoft, UK Fast, Linux Professional Institute and BT. **What's covered in the course?** Secure information technologies form the bedrock of our modern connected mobile society. Our MSci/BSc Cyber Security course will equip you to enter this growing and important industry. The course takes a practice-led approach, making use of equipment and tools found in the industry to give you the best preparation for a successful career. Our approach prioritises the practical skills sought by industry, backing this up with a thorough understanding of theory. The course delivers the latest in computing, network and security technologies, with the opportunity to gain additional accreditation from Cisco, Juniper, Huawei and the Linux Professional Institute. The course delivers a well-rounded curriculum in the security of the communication networks; the security of computer processing and storage equipment and the software that runs on it,

	both private and public, and both local and cloud based; the security and accuracy of information and information systems; and the forensic analysis of threats and attacks, as well as management-level skills such as project and change management, maximising your career potential. Studying computing with us puts you at the heart of an exciting, innovative community. Upon graduation you could progress into a career as a cyber-security engineer, network administrator, and cyber security analyst or network security architect.

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

8	**Derogation from the University Regulations**
	Not applicable

9	Delivery Patterns		
Mode(s) of Study	**Location**	**Duration of Study**	**Code**
BSc (Hons) Full Time	City Centre	3 years	US0937
BSc (Hons) Sandwich Full Time	City Centre	4 years	US0937S
MSci Full Time	City Centre	4 years	UM0044
MSci Sandwich Full Time	City Centre	5 years	UM0044S

10	Entry Requirements	
	Home:	**BSc (Hons) / MSci** At the point of application, you must have GCSE at Grade 4 or above in English Language and Mathematics. Equivalent qualifications will be considered. BBC at A Level or 112 UCAS tariff points from A/AS Level with a minimum of 2 A Levels. At least one from Technology, Mathematics, Science or a Computing related subject. See the website for full details. Students who wish to APEL should contact the course lead to discuss their prior experience or learning. Subject to discussion and appropriateness of the APEL request, the applicant will need to submit an application through the Faculty APEL application process.
	EU:	IELTS 6.0 overall with 5.5 minimum in all bands
	International:	IELTS 6.0 overall with 5.5 minimum in all bands
	Access:	Pass overall with 60 credits, 45 at Level 3 , including a minimum of 12 credits achieved from any Technology units awarded at Merit or Distinction

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, 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
CMP4275	Computer Forensic 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
CMP5355	Software Security	20
CMP5319	Systems Security Attacks and Defences	20
CMP5328	Computer Forensics Tools and Technique	20
CMP5356	Cyber Security Operations	20
CMP5320	Networking Technologies	20
CMP5336	The English Legal System and IT Law	20

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
CMP6211	Advanced Cyber Security Operations	20
CMP6189	Network and Internetwork Forensics	20
CMP6210	Cloud Computing	20

Level 7:

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
CMP7207	Group Integrated Master's Project	40
CMP7170	Information Security Management	20
CMP7167	eDiscovery and Data Analytics	20
CMP7169	Industrial control systems security	20
CMP7164	Advanced Techniques in Digital Forensics	20

12b Structure Diagram

<table>
<tr><td colspan="4">Level 7</td></tr>
<tr><td>Semester 2</td><td rowspan="2">Integrated Masters Project
[40 credits]</td><td>Industrial Control Systems Security
[20 Credits]</td><td>Advanced Techniques in Digital Forensic
[20 Credits]</td></tr>
<tr><td>Semester 1</td><td>Information Security Management
[20 Credits]</td><td>eDiscovery and Data Analytics
[20 Credits]</td></tr>
<tr><td colspan="4">Level 6</td></tr>
<tr><td>Semester 2</td><td rowspan="2">Individual Honours Project
[40 credits]</td><td>Cloud Computing
[20 Credits]</td><td>Ethical Hacking
[20 Credits]</td></tr>
<tr><td>Semester 1</td><td>Advanced Cyber Security Operations
[20 Credits]</td><td>Network and Internetwork Forensics
[20 Credits]</td></tr>
<tr><td colspan="4">Industrial Placement Year (Optional)</td></tr>
<tr><td colspan="4">Level 5</td></tr>
<tr><td>Semester 2</td><td>Cyber Security Operations
[20 Credits]</td><td>System Security Attacks and Defences
[20 Credits]</td><td>Computer Forensics Tools and Technique
[20 Credits]</td></tr>
<tr><td>Semester 1</td><td>Software Security
[20 Credits]</td><td>The English Legal System and IT Law
[20 Credits]</td><td>Networking Technologies
[20 Credits]</td></tr>
<tr><td colspan="4">Level 4</td></tr>
<tr><td>Semester 2</td><td>Computer Forensic Fundamentals
[20 Credits]</td><td>Applied Operating Systems
[20 Credits]</td><td>Network Fundamentals
[20 Credits]</td></tr>
<tr><td>Semester 1</td><td>Computer Programming
[20 Credits]</td><td>Maths for Computing
[20 Credits]</td><td>Computer Systems CMP4267
[20 Credits]</td></tr>
</table>

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	77%
Exam	17%
In-Person	6%

Level 5

Workload

24% time spent in timetabled teaching and learning activity

Activity	Number of Hours
Scheduled Learning	288
Directed Learning	490
Private Study	422
Total Hours	1200

Balance of Assessment

Assessment Mode	Percentage
Coursework	57%
Exam	35%
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	80%
Exam	12%
In-Person	8%

Level 7

Workload

18% time spent in timetabled teaching and learning activity

Activity	Number of Hours
Scheduled Learning	210
Directed Learning	338
Private Study	652
Total Hours	1200

Balance of Assessment

Assessment Mode	Percentage
Coursework	76%
Exam	20%
In-Person	4%