Course Specification

Course Summary Information		
1	**Course Title**	MSc Cyber Security
2	**BCU Course Code**	PT0959
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**
	What's covered in the course? This MSc Cyber Securitycourse provides a broad foundation for Cyber Security concepts while delivering advanced knowledge and skills in key technical areas. Designed to meet the growing demand from global business and industry for robust cyber security systems, this course underpins the principles and practical professional skills you'll need to meet the future challenges faced by organisations, particularly when it comes to strategic security planning. This course provides future Cyber Security professionals with the knowledge and skills needed by the employers. Our strong links with industry enable us to teach the most demanding topics. You will develop 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. Our academic staff members are actively engaged with government and industry to help solve their complex problems. These strong links provide you with plenty of professional opportunities that will help you to acquire valuable exposure to the real life challenges of Cyber Security.

7	**Course Awards**		
7a	**Name of Final Award**	**Level**	**Credits Awarded**
	Master of Science Cyber Security	7	180
7b	**Exit Awards and Credits Awarded**		
	Postgraduate Certificate Cyber Security Postgraduate Diploma Cyber Security	7 7	60 120

8	Derogation from the University Regulations
	Not applicable.

9	Delivery Patterns		
Mode(s) of Study	**Location(s) of Study**	**Duration of Study**	**Code(s)**
Full Time	City Centre	1 years	PT0959
Part Time	City Centre	2 years	PT0960

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 and 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, 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 including legal obligations, regulatory requirements, international standards, ethical considerations, governance, incident response and business continuity plans.
4	Have an appreciation of Cyber Security topics such as network security, digital forensics, information assurance, security testing, threat modelling and secure software development.
Cognitive and Intellectual Skills	
5	Systematically analyse security threats to information assets of an organization, 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 organization against international security standards, such as ISO 27000, identify gaps and recommend mitigations.
7	Apply design principles such as least privileges, fail secure, and defence in depth to engineer security, privacy and resilience by design to a range of case studies.
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 and Professional Skills	

9	Demonstrate the capacity to confidently use digital forensic tools for collecting, analysing, and processing electronic evidence through application of forensically-sound methodologies.
10	Demonstrate hands-on experience on security testing tools, such as penetration testing, to systematically identify certain types of vulnerabilities in communication network infrastructures.
11	Apply a threat modelling tool, such as Microsoft SDL Threat Modelling Tool, to systematically generate and manage potential threats derived from a high level security architecture of an application.
12	Propose a contingency plan, consistent with the organization's view of associated risks, to ensure business continuity for an organization upon the detection of an adverse event.
Key Transferable Skills	
13	Apply skills in research, independent study, self-management, including time management and prioritization 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 to undertake a substantial piece of practical work without close supervision.

12	**Course Requirements**
12a	**Level 7:** ***In order to complete this course a student must successfully complete all the following CORE modules (totalling 180 credits):***

Module Code	Module Name	Credit Value
CMP7170	Information Security Management	20
CMP7169	Industrial Control Systems Security	20
CMP7166	Digital Forensics	20
CMP7175	Software Security and Cloud Security	20
CMP7171	Advanced Ethical Hacking	20
CMP7158	Research Methods and Project Management	20
CMP7200	Individual Master's Project	60

12b Structure Diagram

	MSc Cyber Security (Full Time)		
SEM3	Individual Master's Project 60CR		
SEM2	Industrial Control Systems Security 20CR	Software Security and Cloud Security 20CR	Research Methods and Project Management 20CR
SEM1	Information Security Management 20CR	Digital Forensics 20CR	Advanced Ethical Hacking 20CR

Part-time - September intake only

Year2 SEM3		Individual Master's Project 60CR (submitted January)
Year2 SEM2	Industrial Control Systems Security 20CR	
Year2 SEM1	Advanced Ethical Hacking 20CR	
Year1 SEM2	Research Methods and Project Management 20CR	Software Security and Cloud Security 20CR
Year1 SEM1	Information Security Management 20CR	Digital Forensics 20CR

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 7

Workload

% time spent in timetabled teaching and learning activity

Activity	Number of Hours
Scheduled Learning	288
Directed Learning	436
Private Study	1076
Total Hours	1800

Balance of Assessment

Assessment Mode	Percentage
Coursework	57%
Exam	43%
In-Person	0