Course Specification

MSc Cyber Security

EECT029 (on-campus)

EECT030 (online)

School of Computing, Electronics and Mathematics

Faculty of Engineering, Environment and Computing

Academic Year 2021/22

Please note: This specification provides a concise summary of the main features of the course and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided.

We regularly review our course content, to make it relevant and current for the benefit of our students. For these reasons, course modules may be updated.

More detailed information on the learning outcomes, content, and teaching, learning and assessment methods of each module can be found in the Module Information Directory (MID), student module guide(s) and the course handbook.

The accuracy of the information contained in this document is reviewed by the University and may be verified by the Quality Assurance Agency for Higher Education.

PART A Course Specification

MSc Cyber Security

1. Introduction

The significance of information technology and communication as well as more sophisticated security threats in today's modern society has led to an increasing requirement for people with understanding of the security implications of such technology. This needs improved security skills and high standards for professionalism, while taking into account relevant legal and ethical considerations. In both government and industry we are now seeing a significant demand for cyber security professionals. The MSc in Cyber Security degree will increase students' employment and career opportunities.

The MSc in Cyber Security provides students with the knowledge and necessary skillset in several core areas of cyber security. The programme aims to provide a comprehensive and deep understanding of the security principles as well as the practical techniques used in solving security problems and addressing relevant issues.

The course will provide an opportunity to recent graduates, early- and mid-career practitioners in the computing industry to enhance their knowledge or move into Cyber Security. The course is designed to equip its students to work at a professional level and develop a range of industry-informed knowledge and skills in areas such as network security, secure design, cryptography, risk assessment, ethical hacking, digital forensics and incident response. Running in a research-driven environment, the course will also build foundations for further research at Doctoral level in Cyber security to students from a wider range of undergraduate degrees.

The MSc Cyber Security will be delivered both on-campus and as an online degree course, giving students flexibility to study remotely and at their own time. The delivery is based on a combination of face-to-face sessions and online learning with a substantial element of practical 'hands-on' activities. This is supported by specialist Ethical Hacking, Digital Forensics and Networking laboratories as well as a virtual Cyber Security lab, which are accessible 24/7, providing students the opportunity to apply the theoretical aspects they learn across the course's modules, as well as to design, implement and evaluate a variety of real-world examples and case studies.

A key strength of the Cyber Security courses at Coventry University is the positive interaction between students and staff, and the supportive environment that allows students to develop. Our academic team specialises on several areas of cyber security and is committed to provide academic and technical support to students. The students will be a part of a large community of peers with over 200 Cyber Security and Digital Forensics students, and have the opportunity to participate in activities run by the student-led 'ComSec' club or take part in frequent local and international Capture-the-Flag (CTF) competitions.

Research project opportunities are available for students in order to further develop their skills. Current work covers a range topics such as security for low-powered embedded systems, software defined networking, enhancing security through machine learning, protocol analysis, detecting and analysing steganography, vehicle security and security in Bring-Your-Own-Device (BYOD) environments.

The Cyber Security group has strong links with a number of industries and government bodies, including companies in Cyber Security and Forensics, Automotive, Internet-of-Things (IoT) and others both in supporting our curriculum and learning, as well as research and development addressing real world problems.

Work Placement – On Campus only

For students in today's competitive employment markets having work experience can significantly enhance employment prospects. For this reason, the course offers students the opportunity to undertake a work placement, extending the main provision to a two-year course. The work placement could be International or UK with a focus which may be industry or research. Following a selection process within the first semester and subject to securing an approved placement opportunity, students would move onto the two-year course. International students who are interested in a work placement will be supported in completing an application for extending their Tier 4 visa by international student support services. Upon completion of their placement, students will return to complete the course and the final project for the full award.

2 Available Award(s) and Modes of Study			
Title of Award	Mode of attendance	UCAS Code	FHEQ Level
MSc Cyber Security Fallback Awards PgDip in Cyber Security PgCert Cyber Security	On-campus FT – 1 year 2 years with Work Placement On-campus PT – 2 years Online study is normally 2 to 5 years		7

3 Awarding Institution/Body	Coventry University.
4 Collaboration	N/A
5 Teaching Institution and Location of delivery	Coventry University
6 Internal Approval/Review Dates	Date of approval*/latest review*: May 2018 Date for next review: 2026
7 Course Accredited by	
8 Accreditation Date and Duration	
9 QAA Subject Benchmark Statement(s) and/or other external factors	Designed is accordance with: The Framework for Higher Education Qualifications http://www.qaa.ac.uk/en/Publications/Documents/qualifications-frameworks.pdf Quality Assurance Agency for Higher Education (QAA) Subject Benchmark Statements for Computing http://www.qaa.ac.uk/en/Publications/Documents/SBS-Masters-degree-computing.pdf Aligned with the requirements of **GCHQ** Certification of Master's Degrees in Cyber Security. GCHQ Certification provides assurance of a comprehensive coverage of cyber security in the curriculum as well as confidence in the quality of the course. https://www.ncsc.gov.uk/content/files/protected_files/article_files/Certification-Masters-General-Issue-4-0-01September2016.pdf
10 Date of Course Specification	May 2018
11 Course Director	Dr. Christo Panchev

12 Outline and Educational Aims of the Course

The MSc Cyber Security seeks to provide a post-graduate education covering the main theoretical and practical aspects of the field. The overall aim of the MSc Cyber Security is to provide:

- Deep and comprehensive understanding of the current cyber security issues, concepts and technologies;
- Develop technical skills in assessing systems security, detect and mitigate security incidents;
- Critical awareness of the changing cyber threat landscape and the developments in cyberspace;
- Encourage student to proactively communicate and analyse innovative ideas for addressing current and future security issues in cyberspace;
- Understand and interpret the legal, ethical and social issues in implementing and maintaining systems security.

Additionally, the course would provide a platform for further research at Doctoral level in cyber security to students with a wide range of undergraduate degrees. Furthermore, the course will provide an opportunity to early- and mid-career practitioners in the computing industry to enhance their knowledge or move into Cyber Security.

13 Course Learning Outcomes

A student who successfully completes the course will have achieved the following Course Learning Outcomes.

1. Demonstrate a critical awareness of the legal frameworks, ethical and professional issues of cyber security.
2. Perform systematic risk assessment, identification and analysis in accordance with international standards and demonstrate an ability to deal with complex issues.
3. Demonstrate a comprehensive understanding of network and information systems secure communication technologies and protocols and their application to contemporary Internet-based solutions and technologies.
4. Evaluate and justify a suitable methodology and tools for vulnerability assessment of systems and organisations. Conduct and report an ethically-based security audit and test to a professional standard, recommending and specifying suitable countermeasures.
5. Demonstrate a thorough understanding of the theoretical concepts and implementation of current security frameworks and architectures including secure design methodologies, formal methods, cryptographic protocols and algorithms.
6. Apply appropriate technological solutions and processes in the detection, management and investigation of information security incidents, and document a digital investigation from a legal and professional standpoint.
7. Demonstrate a critical awareness of current issues and new technologies in cyber security which are informed by leading edge research and/or practice in the field.
8. Extrapolate from existing research, scholarship and/or fieldwork findings to identify new or revised approaches to practice.
9. Conduct rigorous research / formal enquiry into cyber security issues that require familiarity with a range of technologies, research sources and appropriate methodologies, and for such to inform the overall learning process.

14 Course Structure and Requirements, Levels, Modules, Credits and Awards

Modules within the course, their status (whether mandatory or options), the levels at which they are studied, their credit value and pre/co requisites are identified in the table below.

Modules will be delivered as a combination of lectures, computer laboratory sessions, online learning, problems classes, seminars discussions and tutorials. The course adopts a combination of lab-rotation model and flipped-classroom of teaching and learning, with a combination of online/in-class lectures, online/in-class tutorials as well as in-class discussions and presentations. These are designed and set by the module leaders reflecting the specific topics with the aim of maximising attainment and learning.

The course structure reflects its main aims and has been designed to match the research interests and expertise of the cyber security academics as well as the latest issues and technologies in cyber security with The National Cyber Security Centre (NCSC) requirements for a master's degree in cyber security curriculum. The core (mandatory) modules provide the critical understanding, comprehensive knowledge and technical skills of the core cyber security areas covered by the course. In semester 2 on-campus students will choose one of the course pathways covering the last two modules of the semester. The Individual project will require the students to perform research into and analysis of the current cyber security issues and undertake a substantial work in addressing those issues.

In semester 2 on-campus students will choose one of the course pathways covering the last two modules of the semester. The Individual project will require the students to perform research into and analysis of the current cyber security issues and undertake a substantial work in addressing those issues.

Pathway A: Cyber Security contains 7026CEM and 7033CEM (on-campus only)
Pathway B: Automotive Security Management contains 7010CEM and 7132CEM (on-campus only)
Pathway C: Cyber Security Technology contains 7010CEM and 7026CEM (on-campus and on-line)
Pathway D: Cyber Security Management 7033CEM and 7132CEM (on-campus only)

Work Placement – On Campus only

During semester 1, students who have expressed an interest in undertaking a work placement should begin the application process for placement opportunities. Students have the responsibility for securing a placement, but they will be supported throughout the application process by a specialist employer engagement team. The university will work with employers to identify opportunities. Subject to securing a placement, the International Student Support team will work with international students to obtain UK study visa extensions. Visas required to work in other countries will be the responsibility of the student.

The course is structured so that students complete two semesters of taught modules and then spend three semesters on placement. During this time students would be enrolled onto modules 7102CEM Extended Masters Work Placement A, 7103CEM Extended Masters Work Placement B and 7104CEM Extended Masters Work Placement C. The modules are zero credit and do not contribute to the classification or name of the award but must be passed to complete the placement. Upon completion of the work placement, students are expected to return to Coventry to complete the final semester during which time they undertake their project module. Successful completion of the Work Placement is reflected in the final student transcript.

Credit level	**Module Code**	**Title**	**Credit Value**	**Mandatory/ Optional**	**Course Learning Outcomes**
Subject to securing an appropriate placement opportunity and fulfilling the selection requirements, students will be transferred to the two-year course and the Work Placement modules listed below are to be taken.					
7	7102CEM	Extended Masters Work Placement A	0	Optional	
7	7103CEM	Extended Masters Work Placement B	0	Optional	
7	7104CEM	Extended Masters Work Placement C	0	Optional	

The work placement is to be taken over three semesters and prior to the final semester of the course.

Cascade of Awards:
MSc Cyber Security: The full curriculum (180 credits).
PgDip in Cyber Security: any 120 credits from the programme of study.
PgCert Cyber Security: any 60 credits from the programme of study excluding 7030CEM.

The delivery patterns in the tables below are an indication and can be subject to change.

Module credit level	**Module Code**	**Title**	**Credit Value**	**Mandatory/ Optional**	**Semester**	**Course Learning Outcomes**
7	7034CEM	Network Security	15	M	1	2, 3
7	7024CEM	Ethical Hacking	15	M	1	1, 2, 4, 7
7	7032CEM	Secure Design and Development	15	M	1	2, 5, 7
7	7031CEM	Cryptography	15	M	1	5, 7
7	7025CEM	Incident Response	15	M	2	1, 2, 3, 6, 7
7	7028CEM	Digital Data Acquisition, Recovery and Analysis	15	M	2	1, 6
7	7026CEM	Security of Emerging Connected Systems	15	M (A, C)	2	1, 3, 7
7	7033CEM	Digital Security Risk and Audit Management	15	M (A, D)	2	1, 2
7	7010CEM	Automotive Cyber Security	15	M (B, C)	2	1, 4, 5
7	7132CEM	Information Security Management	15	M (B, D)	2	1, 2
7	7030CEM	Cyber Security Individual Project	60	M	3	7, 8, 9

Pathway details:

Pathway A: Students must complete: Cyber Security contains 7026CEM and 7033CEM (on-campus only)
The delivery pattern in the tables below is an indication and can be subject to change.

Module credit level	**Module Code**	**Title**	**Credit Value**	**Mandatory/ Optional**	**Semester**	**Course Learning Outcomes**
7	7034CEM	Network Security	15	M	1	2, 3
7	7024CEM	Ethical Hacking	15	M	1	1, 2, 4, 7
7	7032CEM	Secure Design and Development	15	M	1	2, 5, 7
7	7031CEM	Cryptography	15	M	1	5, 7
7	7025CEM	Incident Response	15	M	2	1, 2, 3, 6, 7
7	7028CEM	Digital Data Acquisition, Recovery and Analysis	15	M	2	1, 6
7	7026CEM	Security of Emerging Connected Systems	15	M	2	1, 3, 7
7	7033CEM	Digital Security Risk and Audit Management	15	M	2	1, 2
7	7030CEM	Cyber Security Individual Project	60	M	3	7, 8, 9

Pathway B: Students must complete: Automotive Security Management contains 7010CEM and 7132CEM (on-campus only)
The delivery pattern in the tables below is an indication and can be subject to change.

Module credit level	**Module Code**	**Title**	**Credit Value**	**Mandatory/ Optional**	**Semester**	**Course Learning Outcomes**
7	7034CEM	Network Security	15	M	1	2, 3
7	7024CEM	Ethical Hacking	15	M	1	1, 2, 4, 7

7	7032CEM	Secure Design and Development	15	M	1	2, 5, 7
7	7031CEM	Cryptography	15	M	1	5, 7
7	7025CEM	Incident Response	15	M	2	1, 2, 3, 6, 7
7	7028CEM	Digital Data Acquisition, Recovery and Analysis	15	M	2	1, 6
7	7010CEM	Automotive Cyber Security	15	M	2	1, 4, 5
7	7132CEM	Information Security Management	15	M	2	1, 2
7	7030CEM	Cyber Security Individual Project	60	M	3	7, 8, 9

Pathway C: Students must complete: Cyber Security Technology contains 7010CEM and 7026CEM (on-campus and on-line)
The delivery pattern in the tables below is an indication and can be subject to change.

Module credit level	**Module Code**	**Title**	**Credit Value**	**Mandatory/ Optional**	**Semester**	**Course Learning Outcomes**
7	7034CEM	Network Security	15	M	1	2, 3
7	7024CEM	Ethical Hacking	15	M	1	1, 2, 4, 7
7	7032CEM	Secure Design and Development	15	M	1	2, 5, 7
7	7031CEM	Cryptography	15	M	1	5, 7
7	7025CEM	Incident Response	15	M	2	1, 2, 3, 6, 7
7	7028CEM	Digital Data Acquisition, Recovery and Analysis	15	M	2	1, 6
7	7026CEM	Security of Emerging Connected Systems	15	M	2	1, 3, 7
7	7010CEM	Automotive Cyber Security	15	M	2	1, 4, 5
7	7030CEM	Cyber Security Individual Project	60	M	3	7, 8, 9

Pathway D: Students must complete Cyber Security Management 7033CEM and 7132CEM (on-campus only)
The delivery pattern in the tables below is an indication and can be subject to change.

Module credit level	**Module Code**	**Title**	**Credit Value**	**Mandatory/ Optional**	**Semester**	**Course Learning Outcomes**
7	7034CEM	Network Security	15	M	1	2, 3
7	7024CEM	Ethical Hacking	15	M	1	1, 2, 4, 7
7	7032CEM	Secure Design and Development	15	M	1	2, 5, 7
7	7031CEM	Cryptography	15	M	1	5, 7

7	7025CEM	Incident Response	15	M	2	1, 2, 3, 6, 7
7	7028CEM	Digital Data Acquisition, Recovery and Analysis	15	M	2	1, 6
7	7033CEM	Digital Security Risk and Audit Management	15	M	2	1, 2
7	7132CEM	Information Security Management	15	M	2	1, 2
7	7030CEM	Cyber Security Individual Project	60	M	3	7, 8, 9

15 Criteria for Admission and Selection Procedure

An applicant for all programmes within will normally be expected to possess at least one of the following:

- A minimum of a second class honours degree in a relevant subject such as Computer Science, Mathematics, Physics or Engineering etc.
- A relevant professional qualification of an equivalent level
- A lower qualification plus appropriate and relevant experience at a professional level
- Satisfactory independent evidence of working for several years in a position that would normally be occupied by an honours graduate, in a relevant area (such as the IT sector), which would lead to gaining benefit from the course.

Students whose first language is not English must demonstrate proficiency in the English language equivalent to IELTS 6.5. Alternatively students may be admitted with IELTS 6.0 if they attend and pass a compulsory five week pre-sessional English course, operated by Coventry University, before joining their master's programme.

- Applications from those not possessing the equivalent of an honours degree in computer related subject will be considered on individual merit and decisions will be based on careful evaluation of the capacity of the applicant to complete the programme successfully.
- The programme is subject to the general University admission procedures and access policies. A wide range of academic backgrounds is deemed suitable for entry to the programme. However, careful monitoring of applications to ensure that applicants are suited to the programme takes place. Where necessary and possible, applicants are interviewed, especially those who do not appear to meet standard admissions criteria.
- Accreditation for prior learning (APL) is in accordance with University regulations.
- The accreditation for Prior Experiential learning (APEL) will only be awarded for achievements equivalent to masters' level.

16 Academic Regulations and Regulations of Assessment

This Course conforms to the standard University Regulations Mode R.

17 Indicators of Quality Enhancement

The QAA's Higher Education Review undertaken in February 2015 confirmed that Coventry University meets the UK expectations regarding the:

- setting and maintenance of the academic standards of awards;
- quality of student learning opportunities;
- quality of the information about learning opportunities;
- enhancement of student learning opportunities

The assurance of the quality of modules is the responsibility of the Boards of Study which contribute modules to the courses. The Programme Assessment Board (PAB) for the Faculty of Engineering, Environment and Computing is responsible for considering the progress of all students and making awards in accordance with both the university and course-specific regulations.

Students are represented on the Student Forum, Boards of Study and Faculty Board, all of which normally meet two or three times per year. Student views are also sought through module and course evaluation questionnaires.

External Examiners are appointed for all named University awards. The role of the External Examiner at module level is to ensure that academic standards are in line with national norms for the subject. External Examiners report annually on the programme and their views are considered as part of the Course Quality Enhancement Monitoring report (CQEM). Details of the CQEM process can be found on the Registry's web site.

Lecturers, guest speakers, case studies and web materials are used when appropriate to ensure that the content of the MSc programme remains valid and contemporaneous, drawing on relevant expertise from within the course team. Research activity and interests, relevant scholarly and consultancy activities will be used to inform the module content within the MSc programme.

There is a diverse and active range of research activities influencing programmes in most areas of the Faculty. All staff teaching on the MSc Cyber Security course is actively engaged in research directly related to the content of the module in which they are engaged.

In all areas of the Faculty there is a strong and regular industry input to the subject-base. This is achieved in many ways, for example there are several long-standing advisory boards, through industry-focused collaborative research initiatives and use of guest speakers from industry. Alumni from the course as well as related undergraduate course will be invited to provide feedback, possible student projects as well as engage in guest lectures.

18 Additional Information

Enrolled students have access to additional, key sources of information about the course and student support including:

Student Handbook

Course Handbook

Module Information Directory

CU Online / Moodle

- Module Webs
- Postgraduate Programme Webs
- EC Faculty Postgraduate Web

EEC Student Portal (https://share.coventry.ac.uk/students/EC/Pages/Home.aspx)

Coventry University Student Portal https://share.coventry.ac.uk/students/Pages/Index.aspx

Study Support information is accessible from Student Services (and also from Faculty Registry)

Generic Faculty information is available on the EC Faculty Web

Support is also available via Course Directors, who are available to advise students on academic and pastoral issues. Times that Course Directors are available to meet with students will be shown on course Moodle webs and also their location. Module Leaders and the associated module team are available to offer support at module level. Again module leaders advertise their contact times on module Moodle webs and also their location. Outside of office hours, students can also email any member of academic staff.

The Faculty Registry team support students through their studies, providing information and guidance on the rules and procedures that affect academic progress. Faculty Registry can help students deal with problems they may be having with academic life and help them understand the University's academic processes and regulations. They have a detailed understanding of the curriculum structures and other specialist support that is available within the University.

The Faculty Registry have offices located close to the main Receptions. Students can drop by the Registry support desk which is next to reception in the Engineering and Computing building; Monday – Friday from 1000 – 1600. Or they can contact Registry staff via the Reception desks in the main Engineering and Computing building, the John Laing building or the George Eliot building; Monday – Friday from 0830 – 1700. This team can also be emailed at FacultyRegistry.eec@coventry.ac.uk at any time and this will be passed to each student's dedicated course support team to respond to.

The Faculty Learning Support Co-ordinators work closely with the Disabilities Office in the Hub and Course Teams within the Faculty. Reasonable adjustments will be made for students with disabilities who have registered with the University as requiring additional support with their studies.

The University has an excellent record on widening access and welcomes students from all backgrounds and neighbourhoods with low participation in higher education.

Students have access to a Maths and Stats Support Centre called SIGMA based in the Library as well as the Computer Programming Support and Academic Support (Theta session) at the Engineering and Computing building. The Centre for Academic Writing (CAW) can also provide support on topics ranging from how to organise an academic argument to improving grammar and sentence structure. The university provides support for students' health and wellbeing, which includes a Medical Centre, Spirituality and Faith Centre, Counselling and Mental Health Service, Sports and Recreational Centre and a Nursery.

The Students' Union also provides recreational facilities and support and advice for students. International Students may obtain further help from the student welfare team in the International Student Centre.

There is a careers service where qualified consultants are available to help students think about the issues they face as they move through University studies and prepare for employment.

All students undertaking online courses have access to qualified, subject expect professionals offering support and guidance for the duration of their course. In addition to the Faculty Course Directors and Module Leaders giving direction and focus of studies, Coventry University Online will support students with an allocated Associate Lecturer and when required the support of a Progression Coach.

The Associate Lecturer is an experienced subject expert, trained in using FutureLearn and Online platforms, and will give context to the learning steps, guidance, facilitate learning and aid progression. They will engage with students through live seminar sessions strategically placed at particular pinch points in each module as well as supporting conversation and debate on the FutureLearn platform. The Associate Lecturer will also mark assessments and give 1st stage feedback. In addition the Associate Lecturer, when required in a particular course, will give summative feedback on portfolio building or core strands.

The Progression Coach, a professionally qualified and experienced coach, is available to students who require additional pastoral support and guidance. The Progression Coach can signpost and aid learners who require input from supportive groups such Academic Writing or Welfare. They will also, where required, offer coaching to help students facing challenges to their progressions, challenges such as timetabling studies and preparing for assessments as an example.