UNIVERSITY OF WOLVERHAMPTON

Course Specification

Published Date:	30-Apr-2025
Produced By:	Multi Type Usr Record For All Personnel
Status:	Validated

Core Information

Awarding Body / Institution:	University of Wolverhampton
School / Institute:	School of Engineering, Computing, and Mathematical Sciences
Course Code(s):	CS039P01UM Full-time 12 Months
Course Title:	Master of Research in Cyber Security
Hierarchy of Awards:	Master of Research Cyber Security Postgraduate Diploma Cyber Security Postgraduate Certificate Cyber Security University Statement of Credit University Statement of Credit
Language of Study:	English
Date of DAG approval:	16/Sep/2024
Last Review:	
Course Specification valid from:	2023/4
Course Specification valid to:	2029/0

Academic Staff

Course Leader:	Zeeshan Ahmad
Head of Department:	Dr Consolee Mbarushimana

Course Information

Location of Delivery:	University of Wolverhampton
Category of Partnership:	Not delivered in partnership - Standard Provision
Teaching Institution:	University of Wolverhampton
Open / Closed Course:	This course is open to all suitably qualified candidates.

Entry Requirements:

Entry requirements are subject to regular review. The entry requirements applicable to a particular academic year will be published on the University website (and externally as appropriate e.g. UCAS

Applicants should have or be about to complete:

• A recognised undergraduate or postgraduate degree (or equivalent qualification) in Computer Science or closely related subject from an accredited college, institution or university, equivalent to or higher than a UK Bachelor honours degree qualification.

Or

• If the applicant does not hold a recognised degree or hold an ordinary degree, they should have at least three years of relevant work experience.

English language

If English isn't the applicant's first language, they will need to provide evidence of English language ability. We accept:

- IELTS (Academic) at 6.5 overall with no individual component below 6.0
- Pearson PTE (Academic) overall minimum 50
- Cambridge Certificate of Proficiency in English (CCAE & CPE) with minimum scores of 162 in Listening, Reading, writing and Speaking
- TOEFL iBT overall minimum 60
- Trinity Integrated Skills in English (ISE) II: Merit or Distinction
- IGCSE - ENGLISH AS A SECOND LANGUAGE
- IGCSE - ENGLISH LANGUAGE
- O-Level English Language or GCSE English Language Grade C or above (UK Exam Board) Malaysian SPM 1119 Grade 6 or above.

Distinctive Features of the Course:

The Master of Research in Cybersecurity programme is designed to provide students with advanced knowledge and research skills in the field of cybersecurity. The programme emphasizes research skills development, making it an attractive option for prospective students. Comprehensive training covers research methodologies, data analysis, and critical thinking, ensuring that graduates emerge with the ability to conduct independent, high-quality research. The focus on research skills equips students with a valuable asset sought after both employers and academia. Key aspects of the MRes programme include hands-on research projects, allowing students to contribute to the advancement of cybersecurity knowledge and defence strategies. The programme's interdisciplinary approach prepares graduates to address complex real-world problems, drawing expertise from various disciplines.

The curriculum is designed to provide flexible learning options, with module materials tailored to suit a wide variety of students, including those who are working professionals and international learners. This adaptable approach ensures that students can pursue their academic and career aspirations while accommodating their unique circumstances.

Educational Aims of the Course:

The course aims to provide participants with a strong knowledge of the fundamentals of Cybersecurity,

and to equip them with the competencies and research skills needed to address complex cybersecurity challenges and make significant contributions to the field through research, innovation, and professional practice. First and foremost, the programme aims to foster a deep understanding of advanced research methodologies, equipping students with the skills to plan, execute, and communicate their research effectively. It encourages critical thinking and independent inquiry, enabling students to tackle complex problems with creativity and rigor. Additionally, the programme seeks to promote interdisciplinary collaboration, facilitating the exploration of diverse academic fields and perspectives. Furthermore, it aims to cultivate a global mindset, encouraging students to engage with international research communities and embrace cross-cultural perspectives. Communication and presentation skills are honed to effectively articulate research findings to both technical and non-technical audiences, including writing research papers, delivering presentations, and engaging in academic discourse. Ultimately, the MRes is committed to producing graduates who are well-prepared to excel in their chosen careers, whether in academia, industry, government, or the non-profit sector, and who are capable of contributing valuable insights and innovations in the cyber landscape.

Intakes:

September
January
May

Major Source of Funding:

OTHER FUNDING

Tuition Fees:

Tuition fees are reviewed on an annual basis. The fees applicable to a particular academic year will be published on the University website.

Year	Status	Mode	Amount
2024/5	Overseas	Full Time	£15950.00
2024/5	H	Full Time	£9088.00
2025/6	Overseas	Full Time	£16950.00
2025/6	H	Full Time	£8815.00

PSRB:

None

Course Structure:

January (Full-time)

Module	Title	Credits	Period	Type
7CS111	Foundations of Cybersecurity	30	SEM2	Core
7CS112	Research Methods	30	SEM2	Core
7CS113	Dissertation	120	CRYRA	Core

May (Full-time)

Module	Title	Credits	Period	Type
7CS111	Foundations of Cybersecurity	30	SEM3	Core
7CS112	Research Methods	30	SEM3	Core

May (Full-time)

Module	Title	Credits	Period	Type
7CS113	Dissertation	120	INYR	Core

September (Full-time)

Module	Title	Credits	Period	Type
7CS111	Foundations of Cybersecurity	30	SEM1	Core
7CS112	Research Methods	30	SEM1	Core
7CS113	Dissertation	120	INYR	Core

Please note: Optional modules might not run every year, the course team will decide on an annual basis which options will be running, based on student demand and academic factors, to create the best learning experience.

Learning, Teaching and Assessment

Academic Regulations Exemption:

None.

Reference Points:

UK Quality Code for Higher Education

Qualifications and Credit Frameworks

Subject Benchmark Statements

University Policies and Regulations

Equality Act (2010)

Institute of Information Security Professionals (IISP)

ISC2 Certified Information System Security Professional (CISSP) Common Body of Knowledge (CBK)
British Computing Society (BCS)

National Cyber Security Centre (NCSC).

Overview of Assessment:

Learning Outcomes	Modules

Learning Outcomes	Modules
PGCERT01 Demonstrate a systematic understanding of knowledge, and a critical awareness of current problems and/or new insights, much of which is at, or informed by, the forefront of your academic discipline, field of study or area of professional practice with a conceptual understanding that enables the student: - to evaluate critically current research and advanced scholarship in the discipline. - to evaluate methodologies and develop critiques of them and, where appropriate, to propose new hypotheses.	7CS112 Research Methods
PGCERT02 Demonstrate a comprehensive understanding of techniques applicable to your own research or advanced scholarship and ability to continue to advance your knowledge and understanding, and to develop new skills to a high level.	7CS112 Research Methods
PGCERT03 Demonstrate originality in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry are used to create and interpret knowledge in the discipline.	7CS111 Foundations of Cybersecurity 7CS112 Research Methods
PGCERT04 Ability to deal with complex issues both systematically and creatively, make sound judgements in the absence of complete data, and communicate your conclusions clearly to specialist and non-specialist audiences.	7CS111 Foundations of Cybersecurity 7CS112 Research Methods
PGCERT05 Demonstrate self-direction and originality in tackling and solving problems, and act autonomously in planning and implementing tasks at a professional or equivalent level.	7CS112 Research Methods
PGCERT06 Demonstrate the qualities and transferable skills necessary for employment requiring: - the exercise of initiative and personal responsibility decision-making in complex and unpredictable situations. - the independent learning ability required for continuing professional development.	7CS111 Foundations of Cybersecurity 7CS112 Research Methods
MA01 Demonstrate a breadth of knowledge and understanding in the discipline of cybersecurity and work with key cybersecurity concepts and definitions.	7CS111 Foundations of Cybersecurity
MA02 Demonstrate in-depth understanding and the ability to use modern technologies, techniques and methods in cyber exploitation and defence to develop both technical and management controls and solutions against Information security threats.	7CS111 Foundations of Cybersecurity 7CS113 Dissertation
MA03 Acquire and establish a systematic technical expertise and knowledge in risk assessment methodologies and frameworks and regulatory and legal requirements and compliance within a given organisational context in cybersecurity.	7CS112 Research Methods 7CS111 Foundations of Cybersecurity 7CS113 Dissertation
MA04 Undertake a technical analysis of complex scientific evidence and argumentation independently of current knowledge in the subject matter and apply this in a range of relevant contexts in the cyber space with regards to security and safety.	7CS111 Foundations of Cybersecurity 7CS113 Dissertation

Learning Outcomes	Modules
MA05 Flexibly and autonomously apply knowledge in order to undertake a series of activities related to core aspects of security so as to provide innovative and cost-effective solutions adhering to ethical dimensions codes or practice and existing standards.	7CS111 Foundations of Cybersecurity 7CS113 Dissertation
MA06 Undertake a substantial independent piece of research work that tackles a complex problem in Cybersecurity, using incomplete information and demonstrating your ability to analyse, critically evaluate the scenario and utilize this to develop an appropriate solution.	7CS113 Dissertation

Teaching, Learning and Assessment:

Students will engage in a diverse array of learning activities, including computer-based learning and utilising the University's Virtual Learning Environment (CANVAS) for information and interactive communications. The learning activities will encompass lectures, tutorials (both in smaller groups and one-on-one), workshops, and case studies. Additionally, students will participate in structured laboratory exercises, individual structured assignment-based learning, directed study, and various individual or group exercises. Research project investigations will also be a key component of students’ learning experience.

Additionally, students will be encouraged to critically engage with published materials, partaking in self-assessment exercises and improving their analytical skills through the appraisal of scholarly works. This process will be further enriched by opportunities for collaborative learning, both within peer-group discussions and facilitated interactions with tutors. Regular and timely feedback and support will be provided tutors to help students succeed in the course, and opportunities for additional assistance for students who may need extra support will be provided. Formative feedback will play a pivotal role throughout the learning journey, providing students with timely guidance and constructive criticism aimed at enhancing their understanding of the subject.

Assessment Methods

The assessments in this programme are designed not only to assess students' subject-specific knowledge but also to develop their transferable academic skills such as critical thinking, research methodology, communication, and professionalism. A variety of assessment formats will be used to allow students to demonstrate their knowledge and skills in ways that suit their strengths. Feedback mechanisms are integrated into each assessment to support students' ongoing development and ensure they are well-equipped as competent researchers in cybersecurity.

Assessment Methods:

At the University of Wolverhampton, a variety of modes of assessment will be used to support and test your learning and progress and to help you develop capabilities that are valued beyond your University studies and into your working life. Your course may include a variety of assessment activities:

Written examinations (including online examinations, open and closed book examinations and quizzes)
Coursework (for example, essays, reports, portfolios, project proposals and briefs, CVs, poster presentation)
Practical (for example, oral and video presentations, laboratory work, performances, practical skills assessment)

In the final year of your undergraduate degree, and at the end of your postgraduate degree, you are likely to be expected to write an extended piece of work or research, such as a dissertation or a practice-based piece of research.

Student Support:

General University Support:

The University Library is the key source of academic information for students. The Library provides access to a wide range of online information sources, including e-books, e-journals and subject databases as well as printed material. Our online Library chat service, Library Assist is available 24/7.

The University Library also provides students with academic skills support via the Skills for Learning programme. Students can attend workshops or ask for one-to-one help on a range of skills such as academic writing and referencing. This support is available online and on campus. A range of online skills material is also available at Skills for Learning.

The University also has a host of other services to support you, please take a look at the Student Support website: www.wlv.ac.uk/current-students/student-support/ . If you have any questions, need help or advice then ASK@WLV is there for you: www.wlv.ac.uk/current-students/askwlv/.

Course Specific Support:

The MRes in Cybersecurity will provide access to state-of-the-art research facilities, databases, and collaboration opportunities. These resources underline the programme's commitment to providing students with the best tools and support for their research journey, enabling them to thrive in their studies. Faculty expertise is a crucial asset of the MRes programme. The experienced and accomplished faculty members are dedicated to mentoring and guiding students throughout their research endeavours, offering valuable insights and support along the way.

Flexible and interactive e-learning opportunities are offered to on-line distance learning students. The University VLE provides a platform for learning materials and activities to support students' online learning across all modules. A cohesive pack of online components has been designed to present an integrated package of learning, teaching and support and all e-learners will be supported by online tutors. In addition, e-learners will make use of the online databases and academic skills support available through the Library, as well as IT support and software resources from the University's Digital Services.

The Course Leader will monitor the academic and experiential quality of the Course through Award Boards, focus groups and other channels. The Course Leader also proactively supports and directs students on the Course, both collectively and individually, and responds to inquiries and requests regarding the academic programme of study.

Employability in the Curriculum:

The programme's relevance to various industries, government agencies, and non-profit organisations is a key selling point. Graduates acquire skills and knowledge that are highly sought after in the job market, positioning them as valuable assets capable of making an immediate impact in cybersecurity.

Students on this programme will have a learning journey underpinned by the University's innovative research projects and strong links with industry. Students will have access to the University of Wolverhampton's Cyber Resilience and AI (CYBRAI) Research Centre to learn with a first-hand experience how we address the unique complexity and challenges associated with cybersecurity in a constantly evolving threat landscape.