UNIVERSITY OF WOLVERHAMPTON

Course Specification

Published Date:	17-Aug-2026
Produced By:	Multi Type Usr Record For All Personnel
Status:	Validated

Core Information

Awarding Body / Institution:	University of Wolverhampton		
School / Institute:	School of Architecture, Computing and Engineering		
Course Code(s):	CS069P01UM CS069P31UM	Full-time Part-time	15 Months 28 Months
Course Title:	MSc Cyber Security		
Hierarchy of Awards:	Master of Science Cyber Security		
Language of Study:	English		
Date of first cohort:	14/Sep/2026		
Specification valid from:	2026/7		

Academic Staff

Course Leader:	Oluwafemi Falobi
Head of Department:	

Course Information

Location of Delivery:	University of Wolverhampton
Category of Partnership:	Standard Provision (Not delivered in partnership)
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:

1. 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

Work Experience Pathways:

1. At least 3 years of relevant work experience, demonstrating in-depth knowledge of the sector for the subject matter you are interested in pursuing.

Evidence of industrial certifications in Information security such as CISSP, CEH, BCS will also be considered for suitable candidates with a minimum of 3 years working experience in related industries. All work experience-based applicants will be required to provide a reference detailing your role(s) and responsibilities from your line manager – this would be requested after you have successfully applied. An interview process will also be utilised to verify suitability for the course for candidates with non-standard academic backgrounds but with demonstrable industry experience.

International Applicants

Your qualifications need to be deemed equivalent to the above entry requirements.

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

1. English Language requirements are normally IELTS 6.5 with a minimum of 6.0 in each area (unless otherwise stated) or equivalent accepted qualification https://www.wlv.ac.uk/international/international-academy/english-at-the-international-academy/language-entry-requirements/

1. Please use the following link https://www.wlv.ac.uk/international/ to see the range of English Language Pre-Sessional courses and related Pre-MSc courses offered by the University of Wolverhampton International Academy.

1. For further information relating to overseas qualification, please use the following link https://www.wlv.ac.uk/international/our-locations/your-country/

Distinctive Features of the Course:

MSc Cyber Security prepares students to meet the growing global demand for professionals who can protect digital systems, networks and data in an increasingly complex threat landscape. As cloud computing, mobile technologies, converged applications and connected infrastructures continue to expand, organisations need cyber security specialists who can understand both the technical and strategic dimensions of security. This course is distinctive because it combines advanced technical education with practical experience and professional insight, enabling students to develop the capabilities required for modern cyber security roles.

The course offers a strong balance of cyber defence, exploitation awareness and Governance, Risk and Compliance (GRC), reflecting the interdisciplinary nature of contemporary security practice. Students explore the methods, tools and techniques used to identify vulnerabilities, assess risks, strengthen security controls and respond to evolving threats across systems and infrastructures. Teaching is informed by current research and Professionalism, and students are supported to develop not only specialist technical knowledge, but also critical thinking, decision-making and problem-solving skills.

A standout feature of the course is access to a dedicated virtual cyber security operations environment developed in collaboration with industry to reflect current professional practice and help ensure the skills you develop remain aligned with sector expectations. This gives students valuable experience of working in an environment that reflects real security operations, helping them connect theory to practice and build confidence in handling realistic cyber scenarios. By combining hands-on learning, specialist knowledge and broader professional skills, the course equips graduates for careers across technical, operational, governance and risk-focused areas of cyber security.

Distinctive features include:

- Access to a dedicated virtual cyber security environment for offensive and defensive practice as part of the student learning experience.
- A distinctive curriculum that integrates technical cyber skills with Governance, Risk and Compliance (GRC).
- Coverage of cyber defence operations, offensive security practices, and security risk management to support rounded cyber capability.
- Specialist study in areas such as ethical hacking, Internet of Things security, cyber risk, network defence, incident response and secure systems.
- Hands-on experience with industry tools, technologies and methods used in cyber security practice, scenario-based exercises.
- Research and industry-informed teaching from staff with expertise in cyber security, security operations and applied practice.
- Practical, scenario-based learning that reflects real organisational and infrastructure security challenges.
- A student experience that builds technical confidence, professional networks and long-term employability.
- Preparation for a wide range of cyber security careers in commercial, public sector and critical infrastructure settings.

Intakes:

September

November
January
March

Major Source of Funding:

Office for Students (OFS)

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
2026/7	H	Full Time	£11015.00
2026/7	Overseas	Full Time	£18645.00
2026/7	H	31	£5508.00

PSRB:

None

Course Structure:

January (Full-time)

Module	Title	Credits	Period	Type
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

January (Full-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core

January (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core

January (Part-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core

March (Full-time)

Module	Title	Credits	Period	Type
7CS122	Research Methods & Professionalism	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS122	Research Methods & Professionalism	15	INYR	Core

March (Full-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core

March (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS124	Incident Management and Response	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core

March (Part-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

September (Full-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

September (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

September (Part-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

November (Full-time)

Module	Title	Credits	Period	Type
7CS129	Secure Infrastructure	15	INYR	Core
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS129	Secure Infrastructure	15	INYR	Core
7CS136	Ethical Hacking	15	INYR	Core
7CS122	Research Methods & Professionalism	15	INYR	Core

November (Full-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS141	Information Assurance	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS141	Information Assurance	15	INYR	Core

November (Full-time)

Module	Title	Credits	Period	Type
7CS139	Computer Science Dissertation	60	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS135	Secure Cyber-Physical and IoT Systems	15	INYR	Core
7CC016	Cloud Infrastructure and Platforms	15	INYR	Core
7CS124	Incident Management and Response	15	INYR	Core

November (Part-time)

Module	Title	Credits	Period	Type
7CS137	Generative AI and Automation for Cybersecurity	15	INYR	Core
7CS139	Computer Science Dissertation	60	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

Regulations Exemption:

Section 1.3.1 - Exemption from the standard University Academic Framework allowing for the use of 15 credit taught modules at Level 7.

Reference Points:

UK Quality Code for Higher Education

Qualifications and Credit Frameworks

Subject Benchmark Statements

University Policies and Regulations

Equality Act 2010: guidance - GOV.UK

Apprenticeship Standard

Overview of Assessment:

Learning Outcomes	Modules

Learning Outcomes	Modules
PGCERT01 Critically evaluate key concepts, principles, standards and contemporary issues in cyber security, including information assurance, secure infrastructure, cyber-physical and IoT security, and the emerging role of AI and automation in cyber operations. (Knowing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT02 Apply advanced knowledge and understanding of cyber security technologies, methods and controls to assess threats, vulnerabilities and risks in organisational and technical contexts. (Knowing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT03 Make informed judgements on cyber security problems by considering technical, organisational, legal, regulatory and ethical factors, and communicate your conclusions clearly to specialist and non-specialist audiences. (Doing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS141 Information Assurance
PGCERT04 Demonstrate autonomy and originality in planning and undertaking cyber security tasks, using appropriate tools, frameworks and professional judgement to address complex but bounded problems. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT05 Reflect critically on your own learning and performance, identifying how postgraduate study methods and Professionalism can improve your effectiveness in cyber security. (Being)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS135 Secure Cyber-Physical and IoT Systems 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGCERT06 Demonstrate professional and ethical awareness in the protection of systems, services and information, recognising the responsibilities of cyber security practice in organisational and societal settings. (Being)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGDIP01 Demonstrate critical understanding and evaluation of advanced cyber security theories, research, standards and Professionalism across information assurance, secure infrastructure, cyber-physical and IoT security, ethical hacking, penetration testing, cloud technologies, and incident management. (Knowing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance

Learning Outcomes	Modules
PGDIP02 Integrate and apply specialist cyber security knowledge to analyse, assess and respond to threats, vulnerabilities, risks and incidents in complex, distributed and evolving digital environments. (Knowing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGDIP03 Select and apply appropriate technical, investigative and risk-based methods to address complex cyber security challenges, including those involving incomplete information, uncertainty and rapidly changing threat conditions. (Doing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGDIP04 Communicate well-reasoned cyber security findings, strategies and recommendations effectively and professionally to a range of audiences, using appropriate academic, technical and industry conventions. (Doing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
PGDIP05 Demonstrate self-direction, initiative and originality in solving advanced cyber security problems and in managing substantial independent work at postgraduate and professional level. (Being)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity
PGDIP06 Exercise ethical, legal and professional responsibility in cyber security decision-making and practice, with awareness of the human, organisational and wider societal implications of security actions and interventions. (Being)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS141 Information Assurance
MA01 Demonstrate a systematic and critical understanding of advanced cyber security knowledge, including contemporary threats, defensive and offensive security approaches, governance and assurance frameworks on cyber security practice. (Knowing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation 7CS141 Information Assurance
MA02 Show originality in the application of cyber security knowledge, together with a practical understanding of how research, enquiry and evidence are used to investigate problems and create, interpret and extend knowledge in the discipline. (Knowing)	7CS122 Research Methods & Professionalism 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation

Learning Outcomes	Modules
MA03 Address complex cyber security issues systematically and creatively, making sound judgements in the absence of complete data and producing justified, context-aware and effective solutions for technical and organisational environments. (Doing)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation 7CS141 Information Assurance
MA04 Plan, execute and evaluate substantial independent work to a high professional standard, demonstrating autonomy, critical decision-making and originality in the analysis and resolution of advanced cyber security problems. (Doing)	7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS139 Computer Science Dissertation
MA05 Exercise initiative, leadership and responsibility in complex and unpredictable situations, taking account of ethical, legal, regulatory and professional expectations in cyber security practice and research. (Being)	7CC016 Cloud Infrastructure and Platforms 7CS122 Research Methods & Professionalism 7CS124 Incident Management and Response 7CS129 Secure Infrastructure 7CS135 Secure Cyber-Physical and IoT Systems 7CS136 Ethical Hacking 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation 7CS141 Information Assurance
MA06 Advance your knowledge, skills and professional capability through independent learning, critical reflection and continuing professional development, preparing for specialist practice, leadership or further research in cyber security. (Being)	7CS122 Research Methods & Professionalism 7CS137 Generative AI and Automation for Cybersecurity 7CS139 Computer Science Dissertation

Teaching, Learning & Assessment Strategy/(Learning and Teaching):

Teaching on this course is structured through a block delivery model that supports flexible entry points while still providing a coherent postgraduate learning experience. Because students may begin the course at different points in the academic year, each block is designed to stand as a meaningful stage of study while also contributing to the overall development of your cyber security knowledge and skills. Across the course, you will engage with a broad range of themes, including assurance, governance, secure infrastructure, ethical hacking, cloud technologies, cyber-physical and IoT security, incident response, and research-led professional practice. This structure allows you to build confidence progressively, wherever you begin, and supports your movement towards more advanced analysis, independent enquiry and the dissertation.

You will learn through a mixture of lectures, seminars, workshops, guided laboratory activity, structured tasks, directed reading and independent enquiry. Some sessions focus on introducing frameworks, models and methods. Others are more applied, requiring you to investigate, discuss, test or evaluate cyber security issues in a practical or scenario-led way. The virtual learning environment supports this by providing access to materials, activities and communication that help you prepare for class and continue learning between taught sessions.

The course also develops the broader capabilities needed for success at postgraduate level. You will strengthen your ability to work with technical information, assess evidence, use professional tools, communicate clearly, work collaboratively where appropriate, and manage your own learning effectively. These academic and digital capabilities are developed through the modules themselves.

Professional relevance runs throughout the course. You will work with realistic cyber security situations, industry tools and current security challenges so that academic study is consistently linked to practice. The course also expects you to use digital technologies critically and responsibly, including the ethical use of AI, automation, data and cyber security tools.

Assessment Methods/Assessments:

Assessment is designed to show what you can do with your knowledge, not just what you can remember. Across the course you will complete a range of tasks that reflect the kinds of analysis, communication and judgement expected in professional cyber security roles. This helps create a balanced assessment pattern and gives you the chance to demonstrate your strengths in more than one way.

Depending on the module, you may be assessed through reports, technical analyses, scenario-based investigations, literature-based work, presentations, practical exercises and research tasks. The final stage of the course is the Dissertation, where you will plan and complete a substantial independent piece of work on a cyber security topic. Taken together, these assessments are intended to help you demonstrate critical thinking, structured problem-solving, reasoned argument and the ability to apply cyber security knowledge in context.

Practice and feedback are built into the course. In many modules, workshop tasks, tutor discussion and early developmental activities help you test your understanding before final submission. This is particularly important in a postgraduate course, where assessment often requires analysis, judgement and independence rather than simple recall. Feedback is used to help you improve your methods, strengthen your reasoning and develop confidence over time.

Assessment design also takes account of accessibility and clarity. You will be given clear expectations, guidance and marking criteria. Using different assessment formats across the course supports a wider range of learners and makes it easier to evidence different types of achievement. In several modules, there is also room for you to shape your assessment around a chosen issue, sector or technical focus, helping your work feel more relevant to your interests and career plans.

Further Information for Student:

The MSc Cyber Security has been designed to support a smooth transition into Master's-level study in a way that is structured, flexible and manageable from the outset. We recognise that students may join the course with different academic, technical and professional experience, so the block delivery model is intended to provide a clear and supportive learning journey. The course is organised so that each block offers a coherent and self-contained stage of study, allowing you to begin at any entry point and still build your knowledge and confidence successfully. This means you can engage with the course in a way that feels accessible while still developing the advanced understanding expected at Level 7.

Academic and practical development are built directly into the course. Rather than treating core skills as something separate, modules are designed to strengthen your ability to read critically, write academically, investigate problems, analyse technical issues and communicate professionally as part of your everyday learning. You will engage with a range of teaching and learning approaches, including lectures, small-group teaching, workshops, case-based discussion, lab activities, guided independent study and both individual and collaborative tasks. Together, these approaches are intended to help you progress steadily and with confidence.

Formative tasks appear early in modules so that you can test your understanding before major submissions. Feedback in workshops, laboratory sessions and other taught activities is used to help you identify what is working well, where you need to improve and how to strengthen your work before final assessment. This gradual build-up is designed to support your progress across the course and prepare you for more demanding pieces of work, including the dissertation.

Although the course does not include a required placement, it is closely aligned to professional cyber security practice. Learning is anchored in realistic scenarios, applied technical work, research-led tasks and contemporary security problems. Student feedback is regularly considered in reviewing delivery and support, helping the course remain current, effective and responsive to the student experience.

Currency:

Cyber security is a fast-moving field, so this course is designed to stay current by combining strong academic foundations with content that can be refreshed to reflect new threats, technologies, standards and professional practices. Alongside core areas such as governance, assurance, risk, secure infrastructure and incident response, the course engages with contemporary developments including AI and automation in cyber security, cloud environments, cyber-physical and IoT systems, and modern offensive and defensive security approaches. These are taught in ways that remain connected to current threats, technologies and professional debates. This means the course is not fixed around a static view of the subject; it is intended to remain responsive to the pace of change in the field.

Research is an important part of the course. You will engage with scholarly and professional sources throughout your studies, and later modules place greater emphasis on research design, critical evaluation and independent investigation. This develops your ability to question claims, weigh evidence and build well-supported arguments of your own.

The course also prepares you to think beyond purely technical issues. Questions of ethics, public trust, sustainability, regulation, social responsibility and organisational resilience are part of the way cyber security is approached. In doing so, the course supports the development of the University's Graduate Attributes by helping you become a knowledgeable, professional, digitally fluent and globally aware graduate. Because cyber security connects to law, business, infrastructure, policy and engineering, you will also be encouraged to think across disciplinary boundaries and to remain open to continued professional learning after graduation.

The course is also informed by external industry and professional input so that what you study remains relevant to current practice. This includes engagement with recognised bodies and sources of professional guidance such as ISC2, BCS, and other relevant cyber security and computing communities. Their frameworks, expectations and evolving priorities help shape the wider context in which modules are reviewed and updated, ensuring that the course reflects both academic developments and employer-facing practice.

Personalisation Opportunities:

MSc Cyber Security gives you meaningful opportunities to shape your learning around your own interests, goals and prior experience. While the course provides a strong core in information assurance, secure infrastructure, cyber-physical and IoT security, ethical hacking, cloud technologies, incident response and research, there is still considerable scope for you to explore areas that are most relevant to your ambitions. This means your learning can remain closely connected to the career path or specialist interests you want to pursue.

Across the course, many activities and assessments allow you to choose a topic, system, organisational context or threat environment that matters to you. You may, for example, focus on critical infrastructure, cloud platforms, enterprise environments, smart systems, public services or other digital settings that reflect your interests or professional background. This helps make your work more relevant and allows you to connect academic study to real-world cyber security challenges. The Dissertation offers the strongest opportunity for personalisation, enabling you to investigate a specialist topic in depth and develop a substantial project aligned to your future goals.

You are also supported in shaping your learning through academic guidance from module tutors and your supervisory support during the dissertation. This helps you make informed choices about assessment topics, project ideas and areas for further investigation, while ensuring that your work remains academically rigorous and professionally relevant.

The course is designed to be inclusive and meaningful for a diverse student body. Learning materials, case studies and discussions encourage you to consider different perspectives, organisational contexts and social impacts of cyber security. You are encouraged to draw on your own experiences, reflect on your progress and use feedback to shape your development as an informed and responsible cyber security professional.

Employability in the Curriculum/Employability and Professional Development:

MSc Cyber Security is designed to help you prepare for a wide range of careers in the cyber security field. Employability and professional development are embedded throughout the course so that you can connect academic study with future career ambitions from the start. The curriculum develops knowledge and skills relevant to roles such as information security analyst, penetration tester, incident responder, security consultant, infrastructure security specialist, governance and risk practitioner, security architect and lead auditor.

Professional development is built into the course through applied learning, realistic scenarios, technical exercises, research tasks and professional presentations. You will develop both specialist cyber security expertise and wider transferable skills such as communication, teamwork, critical thinking, problem solving, evidence-based decision-making and independent learning. These are important for success across a wide range of professional settings and help you build a strong and credible professional identity.

The course is informed by current professional practice and designed with awareness of industry expectations. Learning activities and assessments emphasise responsible decision-making, ethical practice, legal and regulatory awareness, and the ability to work effectively with complex technical and organisational problems. Through lab-based work and scenario-driven tasks, you will engage with tools, platforms and methods that reflect contemporary cyber security environments and professional workflows.

You will also have opportunities to reflect on your strengths, act on feedback and build a portfolio of outputs that can support progression into employment or further specialist development. Research Methods and Professionalism and the dissertation are particularly important in helping you plan your next steps, present your work professionally and demonstrate the autonomy expected in postgraduate study and employment. Overall, the course is designed not only to help you gain a qualification, but to support your growth as a confident, capable and professionally aware cyber security graduate.