AAHE
AUSTRALASIAN ACADEMY
OF HIGHER EDUCATION

Master of Cybersecurity

Course Outline

Key facts

Award granted	AAHE course code
Master of Cybersecurity	MCYB
Study level and type	**Credit points**
Postgraduate coursework	96 credit points
Mode of delivery	**Duration***
Blended: scheduled on-campus, face-to-face classes (three hours per week for each unit) with some online content and activities	Full time: 24 months (4 semesters) Part time: 48 months (8 semesters)
CRICOS course code	**Campus**
113872A	Melbourne
Australian Qualifications Framework (AQF)	**Availability**
Upon successful completion, the award conferred is recognised in the AQF at Level 9	Fee-paying domestic and international students
Course Accreditation	
The Master of Cybersecurity will be seeking accreditation by the Australian Computer Society (ACS).	

**International students must study full-time.*

Key dates

Important dates can be found on the AAHE website under Study at AAHE: https://aahe.edu.au/key-dates/,

Fees

Information about tuition fees, other fees and charges and refunds can be found on the AAHE website under Study at AAHE: https://aahe.edu.au/fees/

Course overview

Protecting information and IT infrastructure from complex and evolving cyber-threats is a critical challenge for modern organisations. The responsibility to prevent and respond to cyber-attacks falls to cybersecurity professionals, and global demand for highly trained cybersecurity professionals is at an all-time high and is expected to increase over time.

The Master of Cybersecurity is a two-year full-time coursework degree (96 credit points) aimed at students wanting to gain a professional qualification to develop expert knowledge and skills in the field.

The course is designed to meet the educational needs of students ultimately seeking to transition into or advance in a career as a cybersecurity professional. You will develop a strong capability in analysing, designing and evaluating cybersecurity technologies and management solutions for complex systems and organisations. This will culminate in a capstone unit incorporating work-related experience, giving you an opportunity to apply the knowledge and skills that you have developed throughout the course in a professional context.

The Master in Cybersecurity covers areas of critical importance to operational-level and management-level cybersecurity professionals. It has been designed with input from leading industry professionals and academics in the field of Cybersecurity. Graduates will acquire an education that meets industry standards and expectations and is on a par with some of the best national and international benchmarks in the field of Cybersecurity.

Course learning outcomes

On successful completion of this course, you will be able to:

- apply advanced and specialised knowledge and skills to critically analyse, design, test, implement, evaluate and manage fit-for-purpose and creative solutions to defend information, processes, IT systems, platforms and networks from cyber threat actors in contemporary contexts for professional practice or scholarship
- develop and apply knowledge of research principles and methods to plan, execute and critically reflect on the process and outcomes of a substantial research-based project, capstone experience and/or piece of scholarship applicable to cyber security in real-world contexts
- analyse, evaluate and assess complex cybersecurity issues, risks and vulnerabilities as they relate to the evolving strategic and operational context of organisations, IT systems and communication networks
- design, develop and evaluate strategies, policies, procedures and practices to manage cybersecurity in organisations based on best practice standards and methods
- clearly present a coherent and independent exposition of the method applied, conclusions made, and professional decisions taken on complex theoretical and technical cybersecurity issues to specialist and non-specialist audiences
- demonstrate professional and ethical standards in the application of cybersecurity knowledge and skills while exercising responsibility and accountability for self-learning and professional practice whether working individually or in a team.

AAHE Graduate Attributes

The AAHE Graduate Attributes below are embedded in the curricula and support the students' ability to acquire and apply the knowledge and skills that they need to succeed in their personal and professional lives.

Graduate attribute	An AAHE graduate will:
Disciplinary knowledge and skills	Be able to confidently apply their comprehensive, discipline-specific knowledge and skills in professional practice and real-world contexts.
Global citizenship and perspective	Possess a deep understanding of the impact that their profession has on society and how it can be used for individual, community and global advancement and well-being. They will develop personal values and practices that are ethically grounded and that embrace diversity, fairness and social and environmental responsibility in local and global contexts.
Communication skills	Be aware of and sensitive to specific situations and audiences when presenting and exchanging information, ideas and concepts. They will demonstrate highly developed speaking, listening and writing skills and will be able to influence others with well-articulated and soundly backed analyses and opinions in a respectful, inclusive and constructive manner.
Critical thinking and problem solving	A critical thinker whose curiosity and creativity leads them to question ideas and assumptions, draw upon evidence and analyse complex scenarios as they formulate their own conclusions and innovative solutions to current and future challenges.
Information and Digital literacy	Be able to identify, locate, analyse and use reliable information effectively and create and convey information in appropriate formats and through effective channels. They will be comfortable utilising a range of digital technologies that are needed to live, learn and work in contemporary society.
Self-management and development	Be self-aware and self-directed with the capacity to set priorities, manage time and work independently. They will be confident in their knowledge and skills, but also reflective and continually striving for personal and professional improvement as life-long learners.
Teamwork and collaboration	Have the capacity to engage productively with others and contribute as a member of a team to a common goal. This will be demonstrated by a high order of competency in navigating team dynamics, encouraging the exchange of ideas and viewpoints, facilitating conflict resolution, negotiation skills and taking a lead when required.

Approach to teaching, learning and assessment

The Master of Cybersecurity will develop your knowledge and skills in the discipline, building towards an authentic work integrated learning (WIL) experience that allows you to apply what you have learnt to real world problems in a professional context and environment. It embeds a collaborative and technology-enabled active learning approach that encourages your participation in the learning process, peer to peer learning and ongoing reflection.

Following a thorough orientation, you will participate in small class groups, where you are encouraged to collaborate, exchange ideas, learn from each other and reflect on your learning, both in the classroom and through the collaborative online learning environment.

The typical weekly process begins with you speculating about a problem or scenario that you have been given before the scheduled on-campus, face-to-face class, then actively engage with the class and reflect on the same problem or scenario. Classes themselves are interactive, with regular anonymous polls and multiple-choice questions to encourage active participation. Following the class, you will document your problem-solving process or reflection on the scenario in an online journal. In this way, using the principles of adult learning, you immediately apply your work to problem-solving, and develop into reflective practitioners. The scenarios and problems, along with the class material, are available to you anytime and anywhere through the online learning management system (LMS). You are also encouraged to engage with your peers through multiple opportunities to collaborate and to interact in the classroom and online.

In preparing for major assessments, you will regularly participate in authentic, experiential learning activities. These may be computer laboratory classes, practical exercises such as conducting penetration testing, risk assessment, team-based projects or real-world work integrated learning experiences such as working for a client in an industry project or through a work placement.

AAHE's active learning approach guides the design of units and their content and activities. The assessments build from this approach and are carefully mapped against the unit and course learning outcomes, establishing clear alignment and assuring that the learning outcomes are achieved.

The design of assessments incorporates smaller formative assessment tasks that enable you to receive regular feedback and stay on track, culminating into one or more summative assessments that measure your learning, skills acquisition and the extent to which you are meeting the units' intended learning outcomes.

WIL requirements

This course has a work integrated learning unit that may involve working on an industry project for a real client or undertaking a placement that involves attending a workplace of an approved host organisation. In such cases, you may be required to undertake a police check, working with children check, immunisation check, or other checks as required.

Course structure

Core units

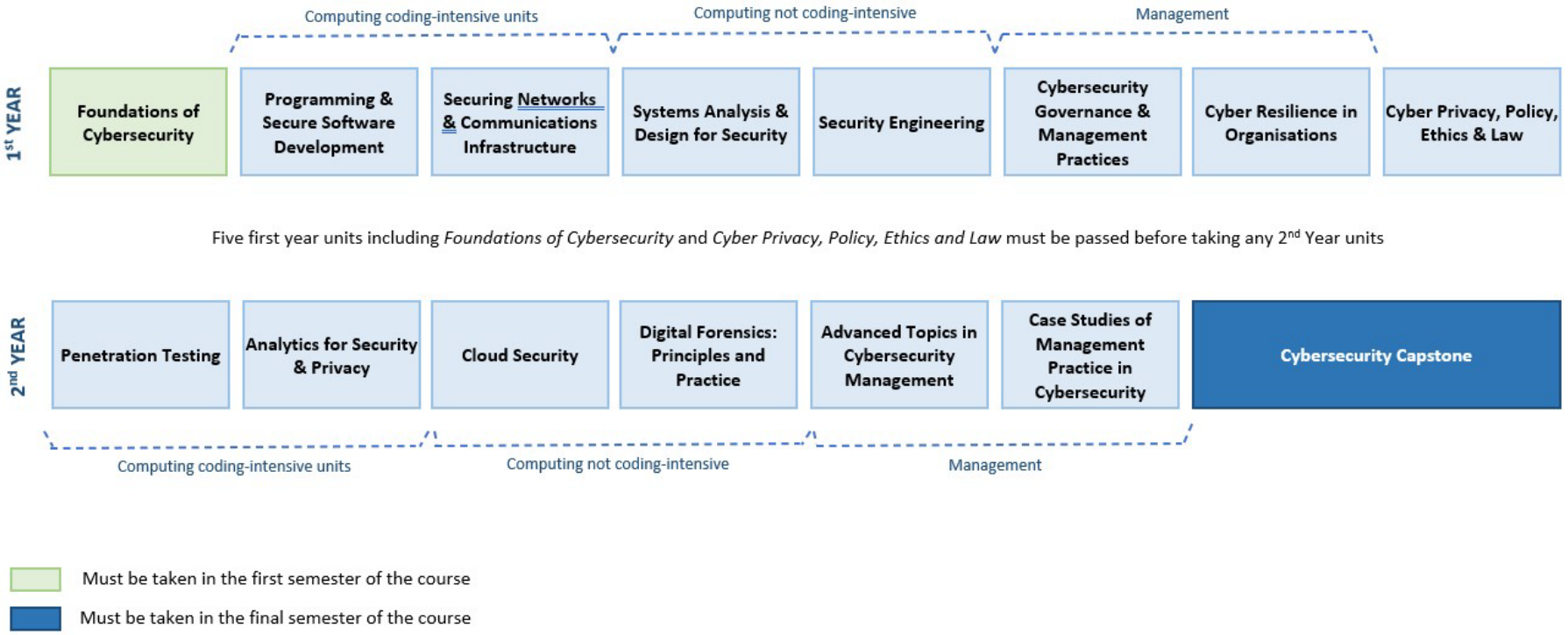
Unit code	Unit title	Credit points
CYB801	Foundations of Cybersecurity	6
CYB802	Programming and Secure Software Development	6
CYB803	Securing Networks & Communications Infrastructure	6
CYB804	Systems Analysis & Design for Security	6
CYB805	Security Engineering	6
CYB806	Cybersecurity Governance and Management Practices	6
CYB807	Cyber Resilience in Organisations	6
CYB808	Cyber Privacy, Policy, Ethics & Law	6
CYB809	Penetration Testing	6
CYB810	Analytics for Security and Privacy	6
CYB811	Cloud Security	6
CYB812	Digital Forensics: Principles and Practice	6
CYB813	Advanced Topics in Cybersecurity Management	6
CYB814	Case Studies of Management Practice in Cybersecurity	6
CYB815	Cybersecurity Capstone	12

Course progression rules

1. All students must take Foundations of Cybersecurity in their first semester of study
2. Five first year units including ***Foundations of Cybersecurity*** and ***Cyber Privacy, Policy, Ethics and Law*** must be passed before any second-year unit may be taken.
3. The capstone unit can only be attempted in the last semester of student candidature and can only be commenced after completion of all first-year units and four second year units.
4. No more than four units may be undertaken in a semester.

See figure below for full details.

Course progression and unit selections



Career outcomes

The Master of Cybersecurity is designed to secure your future professional career in cybersecurity. As a graduate of this course, you will have the requisite knowledge and skills to work in senior operational and management roles in both private and public sector organisations.

The Master of Cybersecurity opens up many opportunities for graduates seeking to enter or advance in the field of Cybersecurity in careers such as:

- Chief Information Security Officers / Director of Cybersecurity / Cybersecurity Practice Lead
- Cybersecurity Operations Coordinator
- Cybersecurity Advisor and Assessor / Cybersecurity Auditor /
- Cyber Threat Analyst
- Intrusion Analyst
- Malware Analyst
- Incident Responder
- Penetration Tester
- Vulnerability Researcher / Vulnerability Assessor

Entry requirements

The Master of Cybersecurity normally consists of 96 credit points; however, up to 48 credit points of credit may be awarded for prior learning or relevant work experience.

Applicants for the 2-year full-time course must have completed a Bachelor degree in any discipline OR 6 years of documented relevant work experience.

Applicants must also meet the minimum English language requirements set out below.

English proficiency

An applicant must provide evidence that they have met the following minimum English language proficiency requirements:

Test	Minimum score
International English Language Testing System (IELTS)	6.5 overall No individual band below 6.0
TOEFL internet-based test taken on or before 25 July 2023	79 overall Reading no less than 19 Writing no less than 24 Speaking no less than 20 Listening no less than 20
C1 Advanced / Cambridge English: Advanced (Certificate in Advanced English)	176 overall No band less than 169
Pearson Test of English Academic (PTE Academic)	56 overall No communicative skill less than 50
Kaplan International Tools for English	459 overall

Only the most recent score from any language proficiency test will be considered and it must be less than two years old on the date the course commences.

Applicants will also be considered to meet the English language requirements if they have successfully completed at least two (2) years of full-time study in English at AQF Level 5 Diploma or above at an Australian registered vocational or higher education provider.

A provisional offer may be made to applicants who provide a Confirmation of Enrolment (COE) for an ELICOS program in English for Academic Purposes (EAP) for a duration of at least twelve (12) weeks for every 0.5 below 6.0 overall or subsection IELTS or equivalent result. Evidence of successful completion of the ELICOS program must be provided before the applicant will be permitted to enrol at AAHE.

The English language proficiency requirement does not apply to applicants in the categories set out in the Migration (English Language Tests and Evidence Exemptions for Subclass 500 (Student) Visa) Instrument (LIN24/022) 2024.

Students who have completed English for Academic Purposes 2 (EAP2 standard) may also be considered to meet the English language requirements but will be assessed on a case-by-case basis.

Applicants who have completed six years of secondary schooling, or a minimum of three years of tertiary education, in an English medium institution in an English-speaking country may be exempted from the English language requirements, unless there is evidence to the contrary.

Applicants from non-English-speaking countries where schooling can be undertaken in English medium institutions can be accepted as having an English-speaking background, provided that they are from an English-speaking community in that country, undertook schooling in an English medium institution and were residents in the country.

Certified copies of evidence of studies undertaken with English as the medium of instruction must be provided before the applicant is permitted to enrol at AAHE.

A list of countries where English is an official language and/or secondary schooling/tertiary education is generally undertaken in English, that is accepted at AAHE, is maintained by the Registrar.

Aboriginal and Torres Strait Islander applicants

Applications from Aboriginal and Torres Strait Islanders who do not meet the entry requirements will be considered on the basis of a personal statement regarding their education and experience and their results in an aptitude test and an interview.

Equipment requirements

Students are required to supply their own laptop and bring it with them to all classes. Due to the technological requirements of this course, it is recommended that students obtain a laptop with the following minimum specifications:

- Intel Core i7
- 32GB of RAM
- Cache Size 12 MB or more
- Primary HDD storage 1TB or more
- Wireless networking IEEE 802.11ac, Bluetooth 5.0
- Operating System: Windows 10 Pro
- USB ports - 3 or more.

Credit for prior learning

Where appropriate, a student whose prior learning or experience exceeds the requirements for admission to AAHE will be granted credit in accordance with the Credit for Learning Undertaken Elsewhere Policy and Procedure. See https://docs.aahe.edu.au/policies/

How to apply

Information about how to apply for the course and the application form can be found on the AAHE website at https://aahe.edu.au/apply//

More information

More information can be found on the AAHE website at https://aahe.edu.au/ or email admissions@aahe.edu.au

AAHE does not guarantee a migration outcome or a successful education assessment outcome to any student who enrols in one of our courses.