Bachelor of Cybersecurity

Course Outline

Australian Qualifications Framework

Key facts

Award granted	**AAHE course code**
Bachelor of Cybersecurity	BCYB
Study level and type	**Credit points**
Undergraduate coursework	144 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: 36 months (6 semesters) Part time: 72 months (12 semesters)
CRICOS course code	**Campus**
113867J	Melbourne
Australian Qualifications Framework (AQF)	**Availability**
Upon successful completion, the award conferred is recognised in the AQF at Level 7	Fee-paying domestic and international students
Pathways to further study	**Course Accreditation**
The Bachelor of Cybersecurity will meet AQF requirements to allow a pathway to postgraduate studies including Graduate Certificate, Graduate Diploma or Master's degree.	The Bachelor 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 Bachelor of Cybersecurity is a three-year full-time course (144 credit points) that provides you with a broad understanding of cybersecurity principles, theory and practice. You will be exposed to real-life case studies on cutting-edge cybersecurity scenarios and trained on state-of-the-art cybersecurity tools and techniques. You will learn to analyse cybersecurity problems and design, implement, evaluate and manage solutions for complex systems and organisations.

The course has been designed with input from leading industry professionals and academics in the field of Cybersecurity, ensuring that you 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.

Specific knowledge and skills that you will gain throughout the course include cybersecurity fundamentals, cyber law, secure software development, cyber risk management, network security and digital forensics. Other areas covered include project management, basic mathematics and computer networking.

In addition to the core subject areas, you can choose electives in specialised units such as critical infrastructure security, embedded systems security and trustworthy systems.

Course learning outcomes

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

- Apply state-of-the-art knowledge and skills to analyse, design, test, implement and manage fit-for-purpose solutions to defend data, processes, IT systems, platforms and networks from cyber threat actors in diverse contexts
- Identify and assess cybersecurity risks and vulnerabilities as they relate to the evolving strategic and operational context of organisations, IT systems and communication networks
- Apply communications and technical skills to interpret cybersecurity requirements and problems and to present a clear, coherent and independent exposition of methods, conclusions and decisions to specialist and non-specialist audiences
- Develop strategies, policies, procedures and practices to manage cybersecurity in organisations based on best practice standards and methods
- Demonstrate professional and ethical standards in the application of cybersecurity knowledge and skills while exercising responsibility and accountability for self-learning and professional practice for both individual and team projects.

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 Bachelor 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 lecture and tutorial 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 portfolio or 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 addition to a mix of interactive lecture and tutorial style learning activities, you will regularly participate in authentic, experiential learning activities. These may be computer laboratory classes, practical exercises such as building a secure network or engaging in an ethical hacking activity, team-based projects or real-world WIL 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 options for work integrated learning units that 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
CYB101	Introduction to Cybersecurity	6
CYB102	Mathematics for Cybersecurity	6
CYB103	Foundations of Programming for Cybersecurity	6
CYB104	Introduction to Computer Networking for Cybersecurity	6
CYB105	Computer Systems and Fundamentals	6
CYB106	Cybersecurity Policy and Law	6
CYB107	Secure Database Design	6
CYB108	Cybersecurity Management	6
CYB201	Systems Analysis for Cybersecurity	6
CYB202	Network Security	6
CYB203	Cryptology	6
CYB204	Secure Applications and DevSecOps	6
CYB205	Machine Learning for Cybersecurity	6
CYB206	Cloud Systems Security	6
CYB207	Embedded Systems and IoT Security	6
CYB208	Cybersecurity Resilience	6
CYB301	Computer Forensics	6
CYB302	Ethical Hacking	6
CYB308	Cybersecurity Capstone Project (work integrated learning unit)	12

Elective units

Unit code	Unit title	Credit points
CYB303	Malware Analysis	6
CYB304	Network Forensics	6
CYB305	Cybercrime, Cyberconflict and Cyberwarfare	6
CYB306	Trustworthy Systems	6
CYB307	Critical Infrastructure Security	6
CYB309	Industry Project (work integrated learning unit)	12
CYB310	Work Placement (work integrated learning unit)	12

Note: *a student can only choose one of either the **Industry Project** or **Work Placement***

Course progression rules

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

See figure on next page for full details.

Course progression and unit selections:

1st YEAR	Introduction to Cybersecurity	Mathematics for Cybersecurity	Foundations of Programming for Cybersecurity	Introduction to Computer Networking for Cybersecurity	Computer Systems and Fundamentals	Cybersecurity Policy and Law	Secure Database Design	Cybersecurity Management
2nd YEAR	Systems Analysis for Cybersecurity	Network Security	Cryptology	Secure Applications and DevSecOps	Machine Learning for Cybersecurity	Cloud Systems Security	Embedded Systems and IoT Security	Cybersecurity Resilience
3rd YEAR	Computer Forensics	Ethical Hacking	Cybersecurity Capstone		• Malware Analysis (6cps) • Network Forensics (6 cps) • Trustworthy Systems (6 cps) • Critical Infrastructure Security (6 cps) • Cybercrime, Cyberconflict and Cyberwarfare (6cps) • Industry Project (12 cps) • Work Placement (12 cps)			

🟩 Must be taken in the first semester of 1st Year

🟦 Must be taken in the first semester of 3rd Year

🟧 Choose units totaling 24 credit points (cps) from the list of electives

Career Outcomes

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

It is anticipated that graduates of this course will work in a diverse range of domains including government, critical infrastructure, supply chain industry, banks and financial institutions, defence and IT firms. It opens up many opportunities for graduates seeking to enter or advance in the field of Cybersecurity in careers (guided by the Australian Signals Directorate skills framework) such as:

Cybersecurity Analysis:

- Cyber Threat Analyst
- Intrusion Analyst
- Malware Analyst

Cybersecurity Operations:

- Incident Response
- Operations Coordinator

Cybersecurity Testing:

- Penetration Testing
- Vulnerability Assessor

Cybersecurity Architecture:

- Cybersecurity Advice and Assessment
- Vulnerability Researcher

Digital Forensics:

- Digital Forensics Investigator

Entry requirements

Applicants must be 18 years or older when they apply for entry.

Applicants must meet the minimum English language requirements set out below, as well as at least one of the following requirements:

- successful completion of an Australian senior secondary qualification (or recognised equivalent)
- successful completion of a qualification at an Australian registered institution of tertiary education, at Australian Qualifications Framework (AQF) level 5 or above
- satisfactory completion of an accredited Tertiary Preparation Program or Foundation Year Program offered by an Australian higher education provider
- a completed or partly completed qualification at AQF Level 6 (Associate Degree) or above from an Australian University or registered Australian higher education provider
- successful completion of a recognised equivalent qualification from another country.

English language requirements

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)	6.0 overall No individual band below 6.0
TOEFL internet-based test taken on or before 25 July 2023	60 overall Reading no less than 13 Writing no less than 21 Speaking no less than 18 Listening no less than 12
C1 Advanced / Cambridge English: Advanced (Certificate in Advanced English)	169 overall No band less than 169
Pearson Test of English Academic (PTE Academic)	50 overall No communicative skill less than 50
Kaplan International Tools for English	426 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.

Mature age applicants

Applicants who are 21 or older and have not completed Year 12 or equivalent will be considered for entry on a case-by-case basis and must either successfully complete a Special Tertiary Admissions Test administered by a tertiary admissions centre or submit a portfolio of their previous work.

Mature age applicants may also be invited to attend an interview with the Dean.

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 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.