Computing and Cyber Security (CDF)

4470  |  144 Units of Credit

Overview

The Bachelor of Computing and Cyber Security (Chief of the Defence Force) is a three-year program at pass level. If eligible, students who have completed the pass degree, may be admitted to an additional one-year Honours program (Program 4517).

The program is designed to build the graduate attributes and skills for market-ready graduates seeking a career in emerging system environments and cyber security engineering, industry, innovation, and research. The program is delivered using state-of-the-art infrastructure for software design, development, networking, security, simulation, testing, and research.

The BCCS(CDF) introduces students to Computer Science fundamentals and builds practical system design and development and cyber security skills. The program builds from foundational topics like programming and systems analysis and design through applications of sophisticated algorithms and techniques for system development and implementation. The focus on Cyber Security develops a broad understanding of cyber security defence, offense and analysis techniques and approaches.

The Bachelor of Computing and Cyber Security (CDF) program develops students’ lifetime skills including creativity, problem-solving ability, critical thinking and communication skills that will be useful not only in a Cyber Security or Cyber war environment but in all professions. It prepares students to deal with technical issues in a computing environment. It develops intellectual and practical problem-solving skills through studies across a range of computing specialisations.
<table>
<thead>
<tr>
<th><strong>Faculty</strong></th>
<th>UNSW Canberra at ADFA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Campus</strong></td>
<td>Canberra</td>
</tr>
<tr>
<td><strong>Study Level</strong></td>
<td>Undergraduate</td>
</tr>
<tr>
<td><strong>Typical duration</strong></td>
<td>3 Years</td>
</tr>
<tr>
<td><strong>Delivery Mode</strong></td>
<td>Face-to-face</td>
</tr>
<tr>
<td><strong>Intake Period</strong></td>
<td>Semester 1</td>
</tr>
<tr>
<td><strong>Academic Calendar</strong></td>
<td>UNSW Canberra Calendar</td>
</tr>
<tr>
<td><strong>Minimum Units of Credit</strong></td>
<td>144</td>
</tr>
<tr>
<td><strong>Award type</strong></td>
<td>Bachelors Pass</td>
</tr>
<tr>
<td><strong>Award(s)</strong></td>
<td>Bachelor of Computing and Cyber Security - BCompCybSec</td>
</tr>
</tbody>
</table>
Learning Outcomes

1. On completion of this program, graduates will be able to apply computational solutions to different verticals in government and industry, by modelling, simulation and integration, following agreed architectures, design standards, patterns, and methodologies, in professional and multi-disciplinary collaboration with identified stakeholders.

2. On completion of this program, graduates will be able to articulate the theoretical underpinnings of information confidentiality, integrity, and availability, including attack lifecycles, cryptography, security controls, ethics, legal aspects, risk assessment, incident response, and standards.

3. On completion of this program, graduates will be able to develop software with appropriate security controls, security implementations, and testing frameworks, implement and configure cyber defensive and offensive technologies, and conduct basic network risk assessments, all in accordance with current best practice and in professional collaboration with the relevant stakeholders.

4. On completion of this program, graduates will be able to provide comprehensive security in existing and new network architectures through intelligent placement of multiple defensive and offensive security controls and systems, based on the different threat profiles faced and the different protections and limitations posed by each.

5. On completion of this program, graduates will be able to articulate ICT disciplinary theories and trends in the current information age, including insights into the ethical and social issues of computing.

6. On completion of this program, graduates will be able to competently demonstrate critical problem-solving and design skills, together with modern project management techniques, in the context of ICT projects.

7. On completion of this program, graduates will be able to work in a productive, ethical, and professional manner – either independently or in teams – applying life-long learning to remain contemporary and competent in the ICT discipline.
8. On completion of this program, graduates will be able to apply the framework of computational thinking and knowledge of computability, complexity theory, and information representation to describe and manipulate fundamental computing knowledge concerning software development and programming languages, operating systems, computer hardware, networks and approaches to refining and maintaining efficiency and security.

9. On completion of this program, graduates will be able to design, implement, verify, validate, document, deploy and explain computational solutions as algorithms coded in high-level programming languages, using conventional standards and tools to meet well-described outcomes.

**Graduate Capabilities:**

For more information on Graduate Capabilities, please click on this [link](link).
**Program Structure**

Students must complete 144 UOC as a standalone program.

The Bachelor of Computing and Cyber Security (CDF) students must complete a minimum 144 UOC comprising:

Core courses - 102 UOC
Discipline Elective courses - 24 UOC
Free Elective courses - 6 UOC
General Education courses - 12 UOC

**Level 1 Core Courses**

Students must take 42 UOC of the following courses.

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>UOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZEIT1102</td>
<td>Introduction to Programming</td>
<td>6</td>
</tr>
<tr>
<td>ZEIT1110</td>
<td>Computer Games</td>
<td>6</td>
</tr>
<tr>
<td>ZEIT1190</td>
<td>Computing and Cyber Security Research 1A</td>
<td>6</td>
</tr>
<tr>
<td>ZEIT1191</td>
<td>Computing and Cyber Security Research 1B</td>
<td>6</td>
</tr>
<tr>
<td>ZINT2100</td>
<td>Introduction to Cyber-Security: Policy &amp; Operations</td>
<td>6</td>
</tr>
<tr>
<td>ZPEM1301</td>
<td>Mathematics 1A</td>
<td>6</td>
</tr>
<tr>
<td>ZPEM1306</td>
<td>Introduction to Discrete Mathematics</td>
<td>6</td>
</tr>
</tbody>
</table>
**Level 2 Core Courses**

Students must take 36 UOC of the following courses.

- ZEIT2102  |  6 UOC  
  Computer Technology

- ZEIT2103  |  6 UOC  
  Data Structures and Representation

- ZEIT2104  |  6 UOC  
  Computers and Security

- ZEIT2106  |  6 UOC  
  Digital Forensics

- ZEIT2190  |  6 UOC  
  Computing and Cyber Security Research 2

- ZPEM2312  |  6 UOC  
  Fundamentals of Data Analysis

**Level 3 Core Courses**

Students must take 24 UOC of the following courses.

- ZEIT3114  |  6 UOC  
  Internetworking

- ZEIT3119  |  6 UOC  
  Web Development and Security

- ZEIT3190  |  6 UOC  
  Computing and Cyber Security Research 3A

- ZEIT3191  |  6 UOC  
  Computing and Cyber Security Research 3B
Level 3 Discipline Electives

Students must take at least 24 UOC of the following courses.

ZBUS3102  |  6 UOC
Project Management

ZBUS3303  |  6 UOC
Logistics Management

ZEIT3113  |  6 UOC
Computer Languages and Algorithms

ZEIT3120  |  6 UOC
Programming for Security

ZEIT3121  |  6 UOC
Securing Networks

ZEIT3404  |  6 UOC
Simulation

**Free Electives**

Students must take at least 6 UOC of the following courses.

any level 1 course

**General Education**

Students must take at least 12 UOC of the following courses.

One of the following:
ZGEN2222  |  6 UOC
Introduction to Strategic Studies

ZGEN2801  |  6 UOC
Strategy, Management and Leadership
One of the following:
ZGEN2215  |  6 UOC  
Law, Force and Legitimacy

ZGEN2240  |  6 UOC  
Introduction to Military Ethics

**Enrolment Disclaimer**

Unless advised otherwise by your program authority, you should follow the rules for the handbook for the year you commenced your program. You are also responsible for ensuring you enrol in courses according to your program requirements. myUNSW enrolment checks that you have met enrolment requirements such as pre-requisites for individual courses but not that a course will count towards your program requirements.
Bachelor of Computing and Cyber Security - BCompCybSec

4427 Computing and Cyber Security

Faculty: UNSW Canberra at ADFA
Campus: Canberra
Units of Credit: 144
Typical Duration: 3 Years

Read More
Admission Requirements

Entry Requirements

A student for enrolment for the degree of Bachelor of Computing and Cyber Security (CDF) shall hold an Australian Tertiary Admission Rank (ATAR) or equivalent of no less than 98.

For more information about admission requirements for various UNSW programs, visit the following website(s):

Domestic Students
International Student
Program Requirements

Progression Requirements

Students in the program must maintain a semester-based WAM of 80 or above.

Students enrolled in the BCompCybSec (CDF) who do not maintain a semester-based WAM of 80 or above will be transferred to the standard BCompCybSec (4427) program with full credit. The specific CDF research project courses completed will be counted as electives within the standard BCompCybSec program.

For more information on university policy on progression requirements please visit Academic Progression.
Pathways

Honours Programs

Bachelor of Computing and Cyber Security (Honours) - BCompCybSec (Hons)
4517 Computing and Cyber Security (Honours)

Faculty: UNSW Canberra at ADFA
Campus: Canberra
Units of Credit: 48
Typical Duration: 1 Years

Read More

Post Graduate

Master of Cyber Security - MCyberSec
8628 Cyber Security

Faculty: UNSW Canberra at ADFA
Campus: Canberra
Units of Credit: 48
Typical Duration: 1 Years

Read More

Master of Cyber Security Operations - MCyberSecOps
8629 Cyber Security Operations

Faculty: UNSW Canberra at ADFA
Campus: Canberra
Units of Credit: 48
Typical Duration: 1 Years

Read More

Master of Cyber Security, Strategy and Diplomacy - MCSSD
8631 Cyber Security, Strategy and Diplomacy

Faculty: UNSW Canberra at ADFA
Campus: Canberra
Units of Credit: 48
Typical Duration: 1 Years

Read More
Recognition of Achievement

University Medal

The University Medal is awarded to recognise outstanding academic performance by a bachelor degree student in line with the University Medal Policy and University Medal Procedure.

Award of Pass with Distinction

The Award of Pass with Distinction is awarded when a weighted average mark (WAM) of at least 75% has been achieved and at least 50% of the requirements of the award completed at UNSW. All eligible programs will award Pass with Distinction except in special circumstances where approval of Academic Board has been given for a program to opt out.

For more information, please visit:

Current Students Pass With Distinction
Additional Information

Program Rules

1. To qualify for the degree of Bachelor of Computing and Cyber Security (CDF), a student shall normally be enrolled for a minimum of six sessions and gain a minimum of 144 UOC (normally 24 UOC in each full time semester). This is composed of 126 UOC of core courses, 6 UOC of free elective courses, and 12 UOC of General Education courses.

2. A student completing a Standard Program shall complete courses, in the years prescribed, for all Computing and Cyber Security (CDF) students as set out in the relevant schedule.

3. A student completing a Non-Standard Program shall, subject to the Requirements of Rule 7 (below), timetabling requirements and the approval of the appropriate Head of School, be permitted to enrol in any one year in courses selected from more than one year of the relevant schedule.

4. Before a student's enrolment will be accepted for any course, the student must have completed the relevant pre-requisite courses shown in the Course Handbook, except where the Course Authority for the appropriate course approves otherwise.

5. A student for enrolment for the degree of Bachelor of Computing and Cyber Security (CDF) shall hold an Australian Tertiary Admission Rank (ATAR) or equivalent of no less than 98.

6. To qualify for the degree of Bachelor of Computing and Cyber Security (CDF), a student shall normally achieve a sessional Weighted Average Mean (WAM) of 85.

7. To remain within the Bachelor of Computing and Cyber Security (CDF) program, a student shall normally maintain a sessional Weighted Average Mean (WAM) of 80.

8. A student of the program Bachelor of Computing and Cyber Security may, at the discretion of the Head of School, transfer to the degree of Bachelor of Computing and Cyber Security (CDF) upon completion of 24 UOC with a WAM of 80 or greater in Semester 1 or 2 of the Year One program.

9. Usually, a student who does not comply with the requirements of Rule 7 (above) shall be transferred to candidature for the degree of Bachelor of Computing and Cyber Security, although exceptions may be made at the discretion of the Head of School. Such review will occur at the end of each semester.
10. Rule 9 (above) shall not usually be invoked for students with potential graduand status.


**Program Fees**

At UNSW fees are generally charged at course level and therefore dependent upon individual enrolment and other factors such as student's residency status. For generic information on fees and additional expenses of UNSW programs, click on one of the following:

- Domestic Students
- Commonwealth Supported Students
- International Students
Pre-2019 Handbook Editions

Access past handbook editions (2018 and prior)

Pre-2019 Handbook Editions
© UNSW Sydney (CRICOS Provider No.: 00098G), 2019. The information contained in this Handbook is indicative only. While every effort is made to keep this information up-to-date, the University reserves the right to discontinue or vary arrangements, programs and courses at any time without notice and at its discretion. While the University will try to avoid or minimise any inconvenience, changes may also be made to programs, courses and staff after enrolment. The University may also set limits on the number of students in a course.

Authorised by Deputy Vice-Chancellor (Academic)
CRICOS Provider Code 00098G
ABN: 57 195 873 179