COURSE OUTLINE

SEC200 Cyber Security

School: School of Science, Technology and Engineering

2026 | Trimester 2

UniSC Sunshine Coast UniSC Moreton Bay UniSC Adelaide	BLENDED LEARNING	Most of your course is on campus but you may be able to do some components of this course online.
Online	ONLINE	You can do this course without coming onto campus, unless your program has specified a mandatory onsite requirement.

Please go to unisc.edu.au for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

Securing data and cyber networks remains one of the most important aspects of modern computing. You will explore key cyber and information security theories, tools and practices including the NIST Cybersecurity Framework and how cyber criminals target individuals and businesses, unlawfully seizing data and identities. You will also identify the dark markets where stolen data, identities and Intellectual Property is traded and how international law enforcement agencies operate to locate and prosecute cyber criminals.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Asynchronous learning material, including videos, articles and review questions	2hrs	Week 1	12 times
Tutorial/Workshop 1 – On campus workshop	2hrs	Week 1	12 times
ONLINE			
Learning materials – Asynchronous learning material, including videos, articles and review questions	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Online workshop	2hrs	Week 1	12 times

1.3. Course Topics

- Cybersecurity,
- Cyber attacks,
- Malicious software,
- Cybersecurity governance,
- Responding to a cybersecurity incident,
- Cybersecurity challenges of the future

2. What level is this course?

200 Level (Developing)

Building on and expanding the scope of introductory knowledge and skills, developing breadth or depth and applying knowledge and skills in a new context. May require pre-requisites where discipline specific introductory knowledge or skills is necessary. Normally, undertaken in the second or third full-time year of an undergraduate programs.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

COURSE LEARNING OUTCOMES On successful completion of this course, you should be able to...		GRADUATE QUALITIES Completing these tasks successfully will contribute to you becoming...
1	Analyse the digital cybersecurity environment from the attacker's and defender's perspectives.	Knowledgeable
2	Explain the range of technical and human-based threats impacting individuals and organisations, and the controls and policies needed to secure against or mitigate them.	Knowledgeable Empowered
3	Rationalise the human and technical vulnerabilities in cyber and information security to understand human reasoning and prevent further attacks.	Creative and critical thinker
4	Justify cyber security and governance practices to manage key cyber scurity risks to an organisation	Empowered
5	Communicate cyber security principles and applications to a variety of technical and non-technical audiences.	Engaged

5. Am I eligible to enrol in this course?

Refer to the UniSC Glossary of terms for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

SEC100

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

SEC301

5.4. Specific assumed prior knowledge and skills (where applicable)

Not applicable

5.5. Microcredential Information

Not applicable

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

On-going formative feedback will be provided in workshops throughout the course.

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Case Study	Individual	35%	1,500 words	Week 5	Online Assignment Submission with plagiarism check
All	2	Case Study	Group	30%	2,500 words	Week 9	Online Assignment Submission with plagiarism check
All	3	Examination - not Centrally Scheduled	Individual	35%	1.5 hour	Week 12	Online Test (Quiz)

All - Assessment Task 1: Cybersecurity Case 1

GOAL:	This task will enable the student to illustrate and articulate cybersecurity strategies and methodologies for a given case scenario.
PRODUCT:	Case Study
AUTHORSHIP STATEMENT:	
FORMAT:	Written report, submitted online
CRITERIA:	

No.		Learning Outcome assessed
1	Identification and explanation of a range of technical and social engineering methodologies	1 2
2	Identification and rationalisation of the human and technical vulnerabilities exploited in cybercrime	3
3	Communication of investigation results	5

GENERIC SKILLS:	Communication, Problem solving, Organisation, Applying technologies, Information literacy

All - Assessment Task 2: Cybersecurity Case 2

GOAL:	Working as a team, students will collectively develop and deliver a structured plan outlining their approach to managing and resolving the cybersecurity scenario provided.
PRODUCT:	Case Study
AUTHORSHIP STATEMENT:	
FORMAT:	Written group report, submitted online

CRITERIA:

No.		Learning Outcome assessed
1	Identification and explanation of a range of technical and social engineering threats, their likelihood and impact on the case study organisation	2 3 4 5
2	Application of control management framework	2 3
3	Development of a business case for senior management	4
4	Professional communication	5

GENERIC SKILLS:	Communication, Collaboration, Problem solving, Organisation, Applying technologies, Information literacy

All - Assessment Task 3: Final exam

GOAL:	The goal of this assessment is measure your understanding and comprehension of cybersecurity.
PRODUCT:	Examination - not Centrally Scheduled
AUTHORSHIP STATEMENT:	
FORMAT:	Final exam completed online via LMS during the final tutorial

CRITERIA:

No.		Learning Outcome assessed
1	Mastery of Cyber security theory and standards	2 3 5
2	Understand basic network structures, protocols, ports and services	1 3 4

GENERIC SKILLS:	Communication, Problem solving, Applying technologies, Information literacy

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Student workload is calculated at 12.5 learning hours per one unit.

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Canvas site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

> There are no required/recommended resources for this course.

8.2. Specific requirements

This course requires access to computers and specialised software which is provided at UniSC campuses for student use. If you elect to do this course online, you may either; attend a campus at which it is available, discuss alternative solutions with your course coordinator that would enable you to demonstrate the learning outcomes, or if you prefer you may acquire this software (if necessary at your own expense). Some software providers may offer discounted or free academic licensing.

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the online induction training for students, and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Canvas, are electronically checked through Turnitin. This software allows for text comparisons to be made between your submitted assessment item and all other work to which Turnitin has access.

10.2. Assessment: Additional Requirements

Eligibility for Supplementary Assessment

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:
(a) The final mark is in the percentage range 47% to 49.4%; and
(b) The course is graded using the Standard Grading scale

10.3. Assessment: Submission penalties

Late submissions may be penalised up to and including the following maximum percentage of the assessment task's identified value, with weekdays and weekends included in the calculation of days late:
(a) One day: deduct 5%;
(b) Two days: deduct 10%;
(c) Three days: deduct 20%;
(d) Four days: deduct 40%;
(e) Five days: deduct 60%;
(f) Six days: deduct 80%;
(g) Seven days: A result of zero is awarded for the assessment task.

The following penalties will apply for a late submission for an online examination:
Less than 15 minutes: No penalty
From 15 minutes to 30 minutes: 20% penalty
More than 30 minutes: 100% penalty

10.4. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Central Examinations
- Deferred Examinations
- Student Conduct
- Students with a Disability

For more information, visit https://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.5. Student Charter

UniSC is committed to excellence in teaching, research and engagement in an environment that is inclusive, inspiring, safe and respectful. The Student Charter sets out what students can expect from the University, and what in turn is expected of students, to achieve these outcomes.

10.6. General Enquiries

For course-specific questions, contact your teaching staff or Course Coordinator.

For other enquiries or to access support, please contact Student Central:

- UniSC Student Central
- UniSC Adelaide Student Central