COURSE OUTLINE

SEC701 Cyber Laws and the Rules of Evidence

School: School of Science, Technology and Engineering

2026 | Trimester 2

UniSC Sunshine Coast 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

This online course will introduce students to cyber security law, and explore how it interacts with other areas of law, including international cyber security law, criminal law, privacy law and the law of evidence. Students will also learn about the jurisdictional and enforcement issues involved in cyber security law. The course will be taught through a combination of online lectures, interactive training modules and reading. By working through the learning modules and completing your assessment tasks, you will become familiar with the legal processes involved in investigating cyber security incidents and will learn to identify and apply the legal principles that relate to cyber security investigations.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Asynchronous Learning Material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – On campus workshop	2hrs	Week 1	12 times
Seminar – On campus seminar	1hr	Week 1	2 times
ONLINE			
Learning materials – Asynchronous learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Online Workshop	2hrs	Week 1	12 times
Seminar – Online seminar	1hr	Week 1	2 times

1.3. Course Topics

Module 1: Cybersecurity and Criminal Law

Module 2: Cybersecurity and Privacy Law

Module 3: Cybersecurity and Evidence Law

2. What level is this course?

700 Level (Specialised)

Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

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	Identify and apply criminal statutes and case laws relating to the lawful seizure, storage and examination of evidence located in an online environment.	Empowered
2	Identify and apply national and international jurisdiction and data sovereignty laws in planning an online investigation.	Empowered
3	Identify and apply privacy laws in a data breach scenario including regulatory compliance with mandatory data breach laws.	Empowered
4	Professionally and ethically respond to case developments and justify actions when managing digital investigations as part of an incident response team.	Empowered
5	Recognise and apply the principles of evidence law in a criminal and privacy context.	Engaged
6	Communicate expert findings to specialist and non-specialist 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

SEC601 or enrolled in SC513

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

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

Using marking rubrics, students will participate in continuous peer and self-assessment during tutorials

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	Quiz/zes	Individual	20%	60 minutes	Week 5	Online Test (Quiz)
All	2	Report	Individual	30%	2000 words	Week 9	Online Assignment Submission with plagiarism check
All	3	Case Study	Individual	50%	4000 words	Week 12	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Cybercrime Test

GOAL:	This online test will consolidate your cyber law knowledge and ensure you have a functional understanding regarding cybercrime and criminal laws.
PRODUCT:	Quiz/zes
AUTHORSHIP STATEMENT:	
FORMAT:	Short answer questions. Timed - one hour (no pauses once started). As this is designed as an online test and it will be open book, you must ensure that you apply strict academic integrity practice while undertaking this assessment.
CRITERIA:	**No.** / **Learning Outcome assessed** 1 Identification and application of jurisdictional issues and other challenges in investigating and prosecuting cybercrime — 1 3 2 Identification and application of relevant provisions of applicable laws, including the Criminal Code Act 1995 (Cth) — 1 3
GENERIC SKILLS:	Problem solving

All - Assessment Task 2: Privacy and Cybercrime Law applications

GOAL:	The goal is to demonstrate your knowledge and understanding of relevant privacy and cybercrime laws, and your ability to apply your knowledge to problem scenarios.
PRODUCT:	Report
AUTHORSHIP STATEMENT:	
FORMAT:	You will be given multiple case studies and you will have to succinctly apply privacy and cybercrime laws and legal principles to each case. Your answers will be short and clearly justified with appropriate references to laws and principles.
CRITERIA:	

No.		Learning Outcome assessed
1	Identification of privacy and cybercrime laws	3
2	Application of the relevant laws and legal principles that apply to a given scenario	5
3	Communication of research using academic writing conventions	6

GENERIC SKILLS:	Communication, Problem solving

All - Assessment Task 3: Criminal and privacy incident case study

GOAL:	The goal of the task is to use your knowledge of criminal, privacy and evidence law to manage a response to a cyber security incident from inception through to a court hearing.
PRODUCT:	Case Study
AUTHORSHIP STATEMENT:	
FORMAT:	This task has been designed as a simulated case study and you will be part of an Incident Response Team. The product is to be a 4,000-word report.
CRITERIA:	

No.		Learning Outcome assessed
1	Management of forensic investigation of the cyber security incident as part of the incident response team	2 4
2	Recognition and protection of legal professional privilege in providing evidence on the cause and consequences of an incident	4 5
3	Recognition and application of the principles of evidence law in a court hearing	5
4	Communication of expert findings	6

GENERIC SKILLS:	Communication, Problem solving, Applying technologies

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 is an online course therefore access to a computer and the internet for 10-12 hours per week is essential.

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