

# SEC701 Cyber Laws and the Rules of Evidence

**School:** School of Science, Technology and Engineering

2022 | Semester 1

Online

ONLINE

You can do this course without coming onto campus.

*Please go to [usc.edu.au](https://usc.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 |
|--|-------|----------------|-----------|
| ONLINE   |       |                |           |
| <b>Learning materials</b> – Asynchronous learning material | 2hrs  | Week 1         | 13 times  |
| <b>Tutorial/Workshop 1</b> – Online Zoom Workshop          | 1hr   | Week 1         | 13 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  |  | GRADUATE QUALITIES   |
|---|--|--|
| On successful completion of this course, you should be able to... |  | 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

Must be enrolled in SC510, SC517, SC513 or SC704

##### 5.2. Co-requisites

Not applicable

##### 5.3. Anti-requisites

Not applicable

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

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 10               | Online Assignment Submission with plagiarism check |
| All           | 3        | Case Study         | Individual          | 50%         | 4000 words                     | Week 13               | Online Assignment Submission with plagiarism check |

### All - Assessment Task 1: Cybercrime Test

|                  |  |                                  |
|------------------|--|----------------------------------|
| <b>GOAL:</b>     | This online test will consolidate your cyber law knowledge and ensure you have a functional understanding regarding cybercrime and criminal laws. 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. |                                  |
| <b>PRODUCT:</b>  | Quiz/zes   |                                  |
| <b>FORMAT:</b>   | Short answer questions. Timed - one hour (no pauses once started)  |                                  |
| <b>CRITERIA:</b> | <b>No.</b>   | <b>Learning Outcome assessed</b> |
|                  | 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                              |

### All - Assessment Task 2: Privacy and Cybercrime Law applications

|                  |   |                                  |
|------------------|---|----------------------------------|
| <b>GOAL:</b>     | 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.   |                                  |
| <b>PRODUCT:</b>  | Report  |                                  |
| <b>FORMAT:</b>   | 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. |                                  |
| <b>CRITERIA:</b> | <b>No.</b>  | <b>Learning Outcome assessed</b> |
|                  | 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                                |

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

|                  |  |                                  |
|------------------|--|----------------------------------|
| <b>GOAL:</b>     | 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. |                                  |
| <b>PRODUCT:</b>  | Case Study   |                                  |
| <b>FORMAT:</b>   | 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.                               |                                  |
| <b>CRITERIA:</b> | <b>No.</b>   | <b>Learning Outcome assessed</b> |
|                  | 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                                |

## 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:

The final mark is in the percentage range 47% to 49.4%

The course is graded using the Standard Grading scale

You have not failed an assessment task in the course due to academic misconduct.

### 10.3. Assessment: Submission penalties

Late submission of assessment tasks may be penalised at the following maximum rate:

- 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task.

- 10% (of the assessment task's identified value) for the third day - 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task.

- A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task. Weekdays and weekends are included in the calculation of days late. To request an extension you must contact your course coordinator to negotiate an outcome.

### 10.4. SafeUniSC

UniSC is committed to a culture of respect and providing a safe and supportive environment for all members of our community. For immediate assistance on campus contact SafeUniSC by phone: [07 5430 1168](tel:0754301168) or using the [SafeZone](#) app. For general enquires contact the SafeUniSC team by phone [07 5456 3864](tel:0754563864) or email [safe@usc.edu.au](mailto:safe@usc.edu.au).

The SafeUniSC Specialist Service is a Student Wellbeing service that provides free and confidential support to students who may have experienced or observed behaviour that could cause fear, offence or trauma. To contact the service call [07 5430 1226](tel:0754301226) or email [studentwellbeing@usc.edu.au](mailto:studentwellbeing@usc.edu.au).

## 10.5. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the [Learning Advisers](#) web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or [studentcentral@usc.edu.au](mailto:studentcentral@usc.edu.au).

## 10.6. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to [Student Hub](#), email [studentwellbeing@usc.edu.au](mailto:studentwellbeing@usc.edu.au) or call 07 5430 1226.

## 10.7. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, [AccessAbility Services](#) can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to [Student Hub](#), email [AccessAbility@usc.edu.au](mailto:AccessAbility@usc.edu.au) or call 07 5430 2890.

## 10.8. 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>

## 10.9. 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.

## 10.10. General Enquiries

### In person:

- **UniSC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **UniSC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **UniSC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **UniSC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **UniSC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **UniSC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

**Tel:** +61 7 5430 2890

**Email:** [studentcentral@usc.edu.au](mailto:studentcentral@usc.edu.au)