Course Outline

Code: SEC701
Title: Cyber Laws and the Rules of Evidence

School:	Science & Engineering
Teaching Session:	Semester 1
Year:	2019
Course Coordinator:	Leah Mooney
Course Moderator:	Professor David Lacey

Please go to the USC website 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 cybersecurity law and explore how it interacts with other areas of law, including international cybersecurity law, criminal law, privacy law and the law of evidence. Students will also learn about the jurisdictional and enforcement issues involved in cybersecurity 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 cybersecurity incidents and will learn to identify and apply the legal principles that relate to cybersecurity investigations.

1.2 Field trips, WIL placements or activities required by professional accreditation

Activity	Details
Nil	Not applicable

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?

Specific Learning Outcomes On successful completion of this course, you should be able to:	**Assessment tasks** You will be assessed on the learning outcomes in task/s:	**Graduate Qualities or Professional Standards mapping** Completing these tasks successfully will contribute to:
Identify and apply criminal statutes and case laws relating to the lawful seizure, storage and examination of evidence located in an online environment.	1, 2, 3	Empowered
Identify and apply national and international jurisdiction and data sovereignty laws in planning an online investigation.	1	Empowered
Identify and apply privacy laws in a data breach scenario including regulatory compliance with mandatory data breach laws.	2, 3	Empowered
Professionally and ethically respond to case developments and justify actions when managing digital investigations as part of an incident response team.	3	Empowered
Recognise and apply the principles of evidence law in a criminal and privacy context.	3	Engaged
Communicate expert findings to specialist and non-specialist audiences.	2, 3	Engaged

5. Am I eligible to enrol in this course?

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

5.1 Enrolment restrictions

Must be enrolled in SC510, SC513, or SC704

5.2 Pre-requisites

Nil

5.3 Co-requisites

Nil

5.4 Anti-requisites

Nil

5.5 Specific assumed prior knowledge and skills (where applicable)

Nil

6. How am I going to be assessed?

6.1 Grading scale

Standard – 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

Task No.	Assessment Product	Individual or Group	Weighting %	What is the duration / length?	When should I submit?	Where should I submit it?
1	Quiz/zes	Individual	20%	60 minutes	Week 5	Quiz (Online Test)
2	Report	Individual	30%	2000 words	Week 10	Online Assignment Submission with Plagiarism check
3	Case Study	Individual	50%	4000 words	Week 13	Online Assignment Submission with Plagiarism check
			100%			

Assessment 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. 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.
Product:	Examination
Format:	Multiple-choice and short answer questions Timed – one hour (no pauses once started)
Criteria:	• Identification and application of jurisdictional issues and other challenges in investigating and prosecuting cybercrime • Identification and application of relevant provisions of applicable laws, including the *Criminal Code Act 1995* (Cth)

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
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:	• Identification of privacy and cybercrime laws • Application of the relevant laws and legal principles that apply to a given scenario • Communication of research using academic writing conventions

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
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:	• Management of forensic investigation of the cyber security incident as part of the incident response team • Recognition and protection of legal professional privilege in providing evidence on the cause and consequences of an incident • Recognition and application of the principles of evidence law in a court hearing • Communication of expert findings

7. What are the course activities?

7.1 Directed study hours

The directed study hours listed here are a portion of the workload for this course. 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. Directed study hours may vary by location. Student workload is calculated at 12.5 learning hours per one unit.

Location:	Directed study hours for location:
Online	This course will take between 10-12 hours per week and may have a combination of: webinar, peer to peer collaboration, asynchronous online materials, and synchronous lecturer zoom meetings.

7.2 Course content

Module	What key concepts/content will I learn?
1 Cybersecurity and Criminal Law	**Course introduction: sources of criminal law and questions of jurisdiction** Identifying relevant offences and applying the act; enforcement of cybercriminal law
2 Cybersecurity and Privacy Law	**Introduction to the *Privacy Act 1988*** Mandatory data breach notification laws; enforcement; monitoring and surveillance
3 Cybersecurity and Evidence Law	**Introduction to evidence law – the *Evidence Act 1995*, types of evidence, questions of jurisdiction, key concepts in evidence law** Questions of admissibility in evidence law; role of accountability in the presentation of evidence in court; international jurisdictions

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

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

8.1 Prescribed text(s) or course reader (Proposed)

Please note that you need to have regular access to the resource(s) listed below as they are required:

Author	Year	Title	Publisher
Gregor Urbas	2015	Cybercrime; Legislation, Cases and Commentary	LexisNexis Butterworths
Dyson Heydon AC	2017	Cross on Evidence	LexisNexis Butterworths
Nigel Phair	2010	Cybercrime: The challenge for the legal profession	eSecurity publishing

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 as a student 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. It is also your responsibility to familiarise yourself with the University's general health and safety principles by reviewing the online Health Safety and Wellbeing training module 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 Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

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%
b) The course is graded using the Standard Grading scale
c) You have not failed an assessment task in the course due to academic misconduct

10.3 Assessment: Submission penalties

Late submission of assessment tasks will 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 and supply the required documentation to negotiate an outcome.

10.4 Study help

In the first instance, you should contact your tutor, then the Course Coordinator. Additional assistance is provided to all students through Academic Skills Advisers. To book an appointment or find a drop-in session go to Student Hub.

Contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au

10.5 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
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website:
http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.6 General Enquiries

In person:

- **USC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **USC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **USC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **USC Fraser Coast -** Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au