COURSE OUTLINE

SEC601 Introduction to Cybersecurity

School: School of Science, Technology and Engineering

2024 | 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.

Please go to 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

In this online course you will be introduced to cybersecurity operations. You will develop the professional knowledge, qualities of thinking and digital collaboration skills needed to prepare you for future technical cyber security courses. You will explore 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 are 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	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Synchronous 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 – Synchronous Zoom workshop	2hrs	Week 1	12 times
Seminar – Online seminar	1hr	Week 1	2 times

1.3. Course Topics

1. Introduction to Cybersecurity
2. Networks and networking
3. Ports, protocols and services
4. The Internet
5. Network vulnerabilities
6. Technical cyber attacks
7. Non-technical & human factors attacks
8. Malicious software
9. Assessing Threats to the Network
10. Cybersecurity governance
11. Responding to a cybersecurity incident
12. Cybersecurity Challenges of the Future

2. What level is this course?

600 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	Describe basic network structures and technologies and how they can be exploited in an organisational context	Knowledgeable
2	Examine the range of technical and human factors (threats and vulnerabilities) that impact networks and the governance and compliance requirements.	Empowered
3	Communicate cyber-security incidents or potential incidents using technical and non-technical language and recommend timely and effective mitigation actions to a broad range of stakeholders.	Engaged
4	Evaluate evolving technologies and the potential cybersecurity implications of their deployment and implementation.	Creative and critical thinker

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

Enrolled in Program SC509 or SC517 or BU708 or SC705

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	Essay	Individual	40%	approx 1,000 words	Week 6	Online Assignment Submission with plagiarism check
All	2	Case Study	Individual and Group	30%	2,500 words	Week 9	Online Assignment Submission with plagiarism check
All	3	Oral and Written Piece	Individual	30%	2,500 words with online references	Week 12	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Weekly Tasks in Aggregate

GOAL:	The goal of this assessment is measure your understanding and comprehension of the Canvas material presented during the week. The tasks may also measure your basic network security knowledge and understanding of cybersecurity principles.
PRODUCT:	Essay
FORMAT:	Students will complete quizzes and answer questions related to the Canvas material
CRITERIA:	

No.		Learning Outcome assessed
1	Demonstration of an understanding of cybersecurity terms and activities	1 2
2	Identification and rationalisation of the human and technical vulnerabilities exploited in cybercrime.	2
3	Expression of creativity, thoughtfulness, and insghtfulness based on an understanding of current information and computing technologies	1 4

All - Assessment Task 2: Cybersecurity Analysis Report

GOAL:	This task will enable the student to identify and articulate technical and human factors attack strategies and methodologies in written format given a scenario of how a notional company operates.
PRODUCT:	Case Study
FORMAT:	You will prepare a written report which will identify weaknesses and vulnerabilities in the protected network of a notional company and how those weaknesses may be exploited by an attacker.

CRITERIA:	No.		Learning Outcome assessed
	1	Analysis of the digital cybersecurity environment	1
	2	Identification and explanation of technical and social engineering methodologies	1 2
	3	Evidence of digital collaboration	3
	4	Discussion of ethics as a function of cybersecurity policies and regulations	2

All - Assessment Task 3: Capture the Flag and Castle Defence

GOAL:	Students will design a defensive or attack strategy for a notional company and present their plan in both a written report and present as a group.
PRODUCT:	Oral and Written Piece
FORMAT:	Given a scenario describing the cybersecurity posture of a notional company, and building on the report they submitted in task 2, students will submit a written plan to attack or defend a protected network. Students will then present their plan to instructors.

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 4
	2	Application of control management framework	1
	3	Development of a business case for senior management	3 4
	4	Communication of results	3
	5	Make recommendations for a network security solution to be implemented by an organisation using the students training and expertise.	1 3 4

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

Please note that you need to have regular access to the resource(s) listed below. Resources may be required or recommended.

REQUIRED?	AUTHOR	YEAR	TITLE	EDITION	PUBLISHER
Recommended	Graeme Edwards	2019	Cybercrime Investigators Handbook	n/a	John Wiley & Sons
Recommended	Thomas J. Holt,Adam M. Bossler,Kathryn C. Seigfried-Spellar	0	Cybercrime and Digital Forensics	n/a	n/a
Required	William Stallings,Lawrie Brown	2017	Computer Security	Fourth	Pearson Higher Education

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. Students should have a device with full administrative rights allowing for the installation of software, browsers, and the ability to navigate to darknet onion URLs.

9. How are risks managed in this course?

Risk assessments have been performed for all field activities and a low level of health and safety risk exists. Some risks concerns may include working in an unknown environment as well as slip and trip hazards. 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 or using the SafeZone app. For general enquires contact the SafeUniSC team by phone 07 5456 3864 or email 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 or email 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.

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 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 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