COURSE OUTLINE

SEC100 Foundations of Computer Security

School: School of Science, Technology and Engineering

2024 | Semester 1

UniSC Sunshine Coast UniSC Moreton Bay	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

With the increase of online and digital presence, the importance of security is becoming more apparent. Through this course you will learn the foundations of computer security including network security, device security and cyber security. This includes identifying the various security threats and developing ethical approaches to mitigate them.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Asynchronous learning material	1hr	Week 1	13 times
Tutorial/Workshop 1 – On campus	2hrs	Week 1	13 times
Seminar – On campus seminar	1hr	Week 1	2 times
ONLINE			
Learning materials – Asynchronous learning material	1hr	Week 1	13 times
Tutorial/Workshop 1 – Online 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 and Device Security
5. Encryption and Network Security
6. Cybercriminals
7. Network Vulnerabilities and Their Exploitation
8. Cyber attack strategies
9. Network Defensive Strategies
10. Investigating the cybersecurity incident
11. Personal cybersecurity
12. Employment opportunities in cybersecurity

2. What level is this course?

100 Level (Introductory)

Engaging with discipline knowledge and skills at foundational level, broad application of knowledge and skills in familiar contexts and with support. Limited or no prerequisites. Normally, associated with the first full-time study year of an undergraduate program.

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 the structure of various networks and devices and the associated security processes and methods necessary to keep them secure	Knowledgeable
2	Compare and contrast the the various components of smart devices and the Internet, the types of information they share, and how they may be exploited by attackers.	Knowledgeable
3	Identify and discuss the ethical, social and societal costs to individuals and the community from security threats	Ethical Sustainability-focussed
4	Analyse and communicate current cybersecurity threats, risks and vulnerabilities to a variety of technical and non-technical audiences.	Engaged
5	Identify and analyse significant cybersecurity challenges that threaten individuals and organisations and make recommendations to mitigate those threats	Knowledgeable Creative and critical thinker 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

Not applicable

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

Students will participate in continuous peer and self-assessment during tutorials and assessments.

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	Written Piece	Individual	20%	1500 word equivalent	Week 5	Online Assignment Submission with plagiarism check
All	2	Oral and Written Piece	Group	40%	1500 words equivalent, PowerPoint presentation delivered as part of a group	Week 10	Online Assignment Submission with plagiarism check
All	3	Portfolio	Individual	40%	50 questions	Exam Period	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Cybersecurity Analysis Report

GOAL:	This task will enable the student to identify and articulate in written format, technical and human factors vulnerabilities identified in a notional company. The assessment will require students to perform detailed analysis of the issues and perform synthesis by associating these vulnerabilities with a variety of attack methodologies. This writing assignment is also designed to introduce you to the art of technical writing. Technical writing is an important part of any professional job where you have to inform management, other employees, or the wider public community of vulnerabilities, exploits and fixes/solutions. This assignment will give you a taste of that environment, and prepare you for further technical writing requirements.
PRODUCT:	Written Piece
FORMAT:	Written report

CRITERIA:

No.		Learning Outcome assessed
1	Educate non technically literate audience about cybersecurity challenges	1 2 3 4
2	Define and prioritise cybersecurity challenge and cybercrimes committed against the public	4
3	Conduct research through Canvas course material and online to identify current cybersecurity threats	3 4
4	Use various Microsoft Office products and applications to present information in a way that educates and informs	4

All - Assessment Task 2: Torchwood: capture the Flag

GOAL:	This assessment is part of a progressive scenario where students will rely on the first assessment to successfully complete this assessment. Given a detailed cybersecurity scenario, each student will assume the role of an attack or a defender as part of a larger group. The scenario describes the cybersecurity posture of a company with national security contracts to a fictitious government. Students will operate in groups of 5 to 7 attackers and will have to devise a series of physical and cyber strategies to either attack and exploit the company using commercially available hacker tools and physical "tiger team" strategies, or, operate as defenders to devise defensive strategies to prevent their company from being successfully attacked using a myriad of physical and cyber defensive strategies. This assessment measures your ability to plan and execute a cybersecurity approach and to present your position to an audience of your peers. In addition to mimicking real-world group decision-making processes and group dynamics, you will have to coordinate your decisions with other decision-makers to execute your plan.
PRODUCT:	Oral and Written Piece
FORMAT:	PowerPoint presentation

CRITERIA:

No.		Learning Outcome assessed
1	Analysis of digital cybersecurity environment	1
2	Communicate and educate a technical and non-technical audience about the cyber-based threats that currently exist.	3 4 5
3	Compare and contrast the various components of smart devices and the Internet, the types of information they share, and how they may be exploited by attackers.	1 4
4	Identify vulnerabilities and methods used to commit a breach in a computer security scenario	1 4

All - Assessment Task 3: Portfolio

GOAL:	To conduct research using Canvas material and online content to answer a series of questions relating to cybersecurity threats, mitigation strategies, policies and procedures, education and training.
PRODUCT:	Portfolio
FORMAT:	The portfolio will consist of 50 questions that can be answered through Canvas and online research

CRITERIA:

No.		Learning Outcome assessed
1	Correctness of answers to provided questions.	1 2 3 4
2	Identify cybersecurity threats	4 5
3	Identify cybersecurity mitigation strategise and appropriate responses to cybersecurity threats	2 4 5
4	Identify components of conventional, mesh, and ad hoc networks	1 2

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	Joseph Migga Kizza	2018	Guide to Computer Network Security	4th	Springer
Required	William Stallings,Lawrie Brown	2017	Computer Security	Fourth	Pearson Higher Education

8.2. Specific requirements

This is a basic, entry level course which does not require any formalised computer or networking experience. To access the course, students need access to a computing device or laptop running a current operating system capable of accessing MS Sway, Canvas, and the Internet. The device should also a graphics card and applicable software able to either play or stream multimedia content.

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

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