School of Information and Physical Sciences

INFT1060: Cybersecurity Fundamentals
Callaghan
Semester 1 - 2024

COURSE OUTLINE

OVERVIEW

Course Description

In this course, you will develop an in-depth introduction to cyber security suitable for all domains of study. You will explore the fundamentals of security, privacy and risk, including core principles, cyber security controls and technologies, policies, procedures, and best practices. Through real world case study examination and assessment based on organisational-focused cyber security frameworks, you will develop a foundational knowledge base in cyber security that can be leveraged and built upon in both academia and industry.

Academic Progress Requirements

Nil

Contact Hours

Callaghan
Computer Lab *
Face to Face On Campus
2 hour(s) per week(s) for 11 week(s) starting Week 2

Lecture
Face to Face On Campus
2 hour(s) per week(s) for 12 week(s)

* This contact type has a compulsory requirement.

Unit Weighting

10

Workload

Students are required to spend on average 120-140 hours of effort (contact and non-contact) including assessments per 10 unit course.

CONTACTS

Course Coordinator	**Callaghan** Dr Geoffrey Skinner Geoff.Skinner@newcastle.edu.au (02) 4985 4512 Consultation: By email appointment.
Teaching Staff	Other teaching staff will be advised on the course Canvas site.
School Office	**School of Information and Physical Sciences** SR233, Social Sciences Building Callaghan CESE-SIPS-Admin@newcastle.edu.au +61 2 4921 5513 9am-5pm (Mon-Fri)

SYLLABUS

Course Content

- An introduction to foundational concepts in cyber security
- Cyber security policy, procedures, and best practices
- Cyber security technologies: hardware and software
- Awareness and management of cyber security, privacy, and risk
- Planning, legal, ethical, and professional issues in information security
- Cyber security maintenance, personnel, and training
- Preparation for the COMPTIA Security+ Certification Exam

Course Learning Outcomes

On successful completion of this course, students will be able to:

1. Apply introductory Cyber Security skills from the perspective of different stakeholders.

2. Identify Cyber Security threats and risks in accordance with organisational processes.

3. Describe how Cyber Security policy and procedure mechanisms support organisations.

4. Explore legal, ethical, and professional issues in the context of Cyber Security.

5. Identify technologies for managing cyber security risks.

Course Materials

Lecture Materials:
- Lecture Slides will be made available prior to the lecture each week.

Multi-Media Resource:
- Recordings of the lecture will be made available shortly after the conclusion of the lecture each week.

Recommended Reading:
- Each week a number of recommended resources will be made available through Canvas.

Required Text:

- Principles of Principles of Information Security, ISBN: 9780357506431
Edition 7, Published: June 2021
Author/s: Michael E. Whitman, J. Mattord

SCHEDULE

ASSESSMENTS

This course has 3 assessments. Each assessment is described in more detail in the sections below.

	Assessment Name	Due Date	Involvement	Weighting	Learning Outcomes
1	Technical Report	11:59pm on Friday the 12th of April (Week 7).	Individual	20%	1, 2, 5
2	A Framework Report	11:59pm on Friday the 7th of June (Week 13).	Group	40%	1, 2, 3, 4, 5
3	Formal Examination	During formal exam period at end of Semester.	Individual	40%	1, 2, 3, 4, 5

Late Submissions   The mark for an assessment item submitted after the designated time on the due date, without an approved extension of time, will be reduced by 10% of the possible maximum mark for that assessment item for each day or part day that the assessment item is late. Note: this applies equally to week and weekend days.

Assessment 1 - Technical Report

Assessment Type   Written Assignment
Purpose   Learning outcomes 1,2,3,4.
Description   An individual technical report paper on a chosen topic within the Cyber Security Domain.
Weighting   20%
Length   4000+ words
Due Date   11:59pm on Friday the 12th of April (Week 7).
Submission Method   Online
Digital submission through Canvas course site.
Assessment Criteria   A marking guide and rubric will be provided with the Assessment handout.
Return Method   Online
Feedback Provided
Opportunity to Reattempt   Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 2 - A Framework Report

Assessment Type   Written Assignment
Purpose   Learning outcomes 1,2,3,4
Description   This is a group project to design, develop, and implement a comprehensive Cybersecurity set of Frameworks, Policies and Procedures for use in a chosen Organization/Company/Industry Sector.
Weighting   40%
Length   5000+ words
Due Date   11:59pm on Friday the 7th of June (Week 13).
Submission Method   Online

Assessment Criteria	Digital submission through Canvas course site. A marking guide and rubric will be provided with the Assessment handout.
Return Method	Online
Feedback Provided	
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 3 - Formal Examination

Assessment Type	Formal Examination
Purpose	Learning outcomes 1,2,3.
Description	Formal exam held in the final exam period.
Weighting	40%
Length	2 hours
Due Date	During formal exam period at end of Semester.
Submission Method	Formal Exam
Assessment Criteria	Examination of the theoretical content of the course.
Return Method	Online
Feedback Provided	
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

ADDITIONAL INFORMATION

Grading Scheme

This course is graded as follows:

Range of Marks	Grade	Description
85-100	High Distinction (HD)	Outstanding standard indicating comprehensive knowledge and understanding of the relevant materials; demonstration of an outstanding level of academic achievement; mastery of skills*; and achievement of all assessment objectives.
75-84	Distinction (D)	Excellent standard indicating a very high level of knowledge and understanding of the relevant materials; demonstration of a very high level of academic ability; sound development of skills*; and achievement of all assessment objectives.
65-74	Credit (C)	Good standard indicating a high level of knowledge and understanding of the relevant materials; demonstration of a high level of academic achievement; reasonable development of skills*; and achievement of all learning outcomes.
50-64	Pass (P)	Satisfactory standard indicating an adequate knowledge and understanding of the relevant materials; demonstration of an adequate level of academic achievement; satisfactory development of skills*; and achievement of all learning outcomes.
0-49	Fail (FF)	Failure to satisfactorily achieve learning outcomes. If all compulsory course components are not completed the mark will be zero. A fail grade may also be awarded following disciplinary action.

*Skills are those identified for the purposes of assessment task(s).

Attendance	Attendance/participation will be recorded in the following components: - Computer Lab (Method of recording: Digital check-in and confirmation with Lab demonstrator.)
Communication Methods	Communication methods used in this course include: - Canvas Course Site: Students will receive communications via the posting of content or announcements on the Canvas course site. - Email: Students will receive communications via their student email account.

Course Evaluation	Each year feedback is sought from students and other stakeholders about the courses offered in the University for the purposes of identifying areas of excellence and potential improvement.
Oral Interviews (Vivas)	As part of the evaluation process of any assessment item in this course an oral examination (viva) may be conducted. The purpose of the oral examination is to verify the authorship of the material submitted in response to the assessment task. The oral examination will be conducted in accordance with the principles set out in the Oral Examination (viva) Procedure. In cases where the oral examination reveals the assessment item may not be the student's own work the case will be dealt with under the Student Conduct Rule.
Academic Misconduct	All students are required to meet the academic integrity standards of the University. These standards reinforce the importance of integrity and honesty in an academic environment. Academic Integrity policies apply to all students of the University in all modes of study and in all locations. For the Student Academic Integrity Policy, refer to https://policies.newcastle.edu.au/document/view-current.php?id=35.
Adverse Circumstances	The University acknowledges the right of students to seek consideration for the impact of allowable adverse circumstances that may affect their performance in assessment item(s). Applications for special consideration due to adverse circumstances will be made using the online Adverse Circumstances system where: 1. the assessment item is a major assessment item; or 2. the assessment item is a minor assessment item and the Course Co-ordinator has specified in the Course Outline that students may apply the online Adverse Circumstances system; 3. you are requesting a change of placement; or 4. the course has a compulsory attendance requirement. Before applying you must refer to the Adverse Circumstance Affecting Assessment Items Procedure available at: https://policies.newcastle.edu.au/document/view-current.php?id=236
Important Policy Information	The Help button in the Canvas Navigation menu contains helpful information for using the Learning Management System. Students should familiarise themselves with the policies and procedures at https://www.newcastle.edu.au/current-students/respect-at-uni/policies-and-procedures that support a safe and respectful environment at the University.

Graduate Profile Statements – Information Technology (UG)

The following table illustrates how this course contributes towards building the skills students will need to work in their profession.

Level of capability
- Level 1 indicates an introduction to a topic at a university level.
- Levels 2 and 3 indicate progressive reinforcement of that topic.
- Level 4 indicates skills commensurate with a graduate – entry to professional practice.

	University of Newcastle Bachelor Information Technology Graduate Profile Statements	Taught	Practised	Assessed	Level of Capability
1	Demonstrate a comprehensive understanding of the discipline of information technologies with an emphasis on net-centric applications, information management, and user requirements for ethical professional practice.	x	x	x	1
2	Apply critical reasoning and systems thinking to understand and support the operation and constraints of contemporary enterprises and their dynamic environment.				
3	Work independently and collaboratively to locate, manage and organise information and resources and apply evidence-based methodologies to create, modify and maintain designs and design solutions.	X	X	X	1

4	Use creativity, problem solving skills, project management skills and technical expertise to analyse, interpret, evaluate and generate solutions to complex technical and organisational problems.				
5	Demonstrate professional judgement and responsibility by communicating information technology principles, practices, standards to specialist and non-specialist audience clearly and persuasively.	X	X	X	1

This course outline was approved by the Head of School. No alteration of this course outline is permitted without Head of School approval. If a change is approved, students will be notified and an amended course outline will be provided in the same manner as the original.